FQ5-547 JP JPO ref 1.

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（A）　(11)特許出願公開番号

特開平10－161935

(43)公開日　平成10年(1998) 6月19日

(51)Int.Cl.[6]		識別記号	FI		
G06F	12/14	320	G06F	12/14	320B
	15/00	330		15/00	330A
H04Q	7/34		H04B	7/26	106A
	7/38				109R
H04L	9/10		H04L	9/00	621Z

審査請求　未請求　請求項の数12　ＯＬ　（全 30 頁）　最終頁に続く

(21)出願番号　特願平9－232934

(22)出願日　平成９年(1997) ８月28日

(31)優先権主張番号　特願平8－248244

(32)優先日　平８(1996) ９月19日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　島川　和典
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内

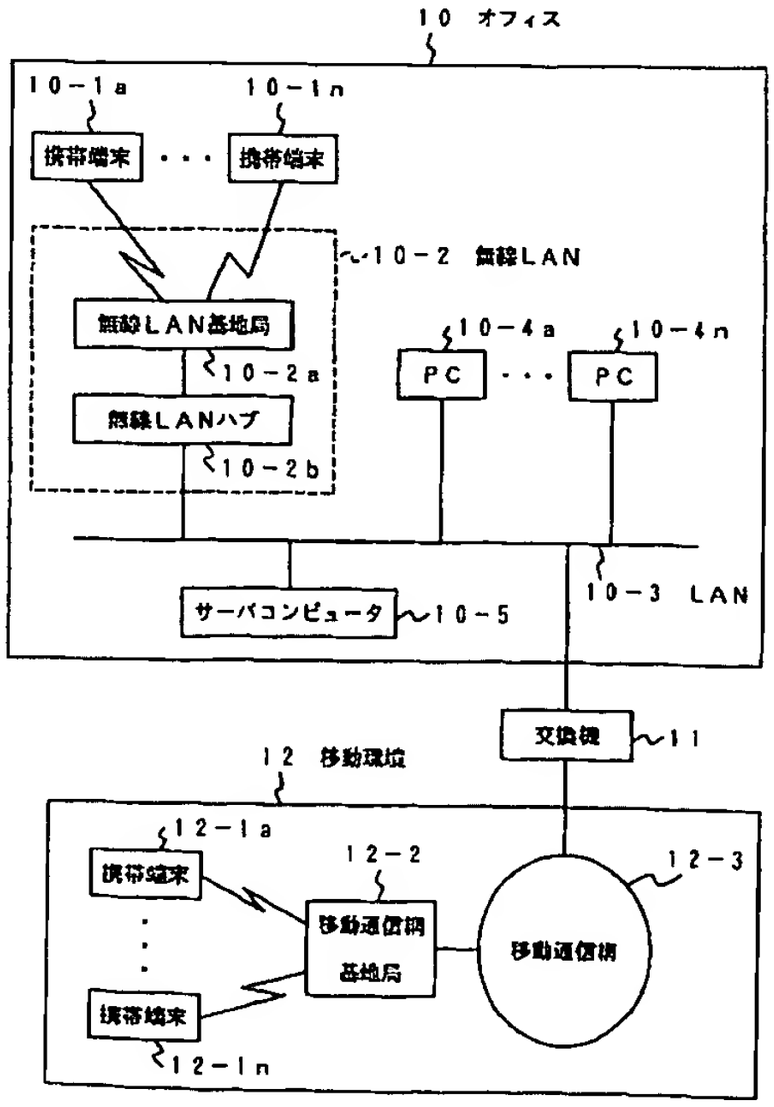
(74)代理人　弁理士　鈴江　武彦　（外６名）

(54)【発明の名称】　セキュリティシステム及びセキュリティ方法

(57)【要約】

【課題】携帯端末上のデータの暗号化／復号化を簡単に行うことができ、操作者に負担を掛けることなく、また、利便性に欠くことなくデータを保護する。

【解決手段】携帯端末１０－１ａは非暗号データ記憶用メモリと暗号データ記憶用メモリを有する。オフィス１０から移動環境１２に移動するとき、操作者によって指定された暗号キーに従って非暗号データ記憶用メモリの非暗号データを暗号化する。この暗号化データを暗号データ記憶用メモリに書き込み、データのアクセス対象を暗号データ記憶用メモリとして暗号モードを設定する。一方、移動環境１２からオフィス１０に戻るとき、操作者によって指定された復号キーに従って暗号データ記憶用メモリの暗号データを復号化する。この復号化データつまり非暗号データを非暗号データ記憶用メモリに書き込み、データのアクセス対象を非暗号データ記憶用メモリとして暗号モードを設定する。



【特許請求の範囲】

【請求項１】　オフィスまたは移動環境で使用され、非暗号データを記憶するための非暗号データ記憶手段と暗号データを記憶するための暗号データ記憶手段とを有する携帯端末と、

この携帯端末を上記オフィスから上記移動環境に移動させるとき、暗号キーを指定する暗号キー指定手段と、

この暗号キー指定手段によって指定された上記暗号キーに従って上記非暗号データ記憶手段から上記非暗号データを読み出し、これを暗号化する暗号化手段と、

この暗号化手段によって暗号化されたデータを上記暗号データ記憶手段に書き込み、データのアクセス対象を上記暗号データ記憶手段として暗号モードを設定する暗号モード設定手段と、

上記携帯端末を上記移動環境から上記オフィスに移動させるとき、復号キーを指定する復号キー指定手段と、

この復号キー指定手段によって指定された上記復号キーに従って上記暗号データ記憶手段から上記暗号データを読み出し、これを復号化する復号化手段と、

この復号化手段によって復号化されたデータを上記非暗号データ記憶手段に書き込み、データのアクセス対象を上記非暗号データ記憶手段として非暗号モードを設定する非暗号モード設定手段とを具備したことを特徴とするセキュリティシステム。

【請求項２】　ネットワークに共有化または非共有化され、非暗号データを記憶するための非暗号データ記憶手段と暗号データを記憶するための暗号データ記憶手段とを有する携帯端末と、

この携帯端末をネットワークに非共有化するとき、暗号キーを指定する暗号キー指定手段と、

この暗号キー指定手段によって指定された上記暗号キーに従って上記非暗号データ記憶手段から上記非暗号データを読み出し、これを暗号化する暗号化手段と、

この暗号化手段によって暗号化されたデータを上記暗号データ記憶手段に書き込み、データのアクセス対象を上記暗号データ記憶手段として暗号モードを設定する暗号モード設定手段と、

上記携帯端末をネットワークに共有化するとき、復号キーを指定する復号キー指定手段と、

この復号キー指定手段によって指定された上記復号キーに従って上記暗号データ記憶手段から上記暗号データを読み出し、これを復号化する復号化手段と、

この復号化手段によって復号化されたデータを上記非暗号データ記憶手段に書き込み、データのアクセス対象を上記非暗号データ記憶手段として非暗号モードを設定する非暗号モード設定手段とを具備したことを特徴とするセキュリティシステム。

【請求項３】　無線環境下でオフィスまたは移動環境で使用され、非暗号データを記憶するための非暗号データ記憶手段と暗号データを記憶するための暗号データ記憶手段とを有する携帯端末と、

この携帯端末が受信する電波が上記オフィスに特有のものか上記移動環境に特有のものかを検出する電波検出手段と、

この電波検出手段によって上記移動環境に特有の電波が検出されたとき、暗号キーを指定する暗号キー指定手段と、

この暗号キー指定手段によって指定された上記暗号キーに従って上記非暗号データ記憶手段から上記非暗号データを読み出し、これを暗号化する暗号化手段と、

この暗号化手段によって暗号化されたデータを上記暗号データ記憶手段に書き込み、データのアクセス対象を上記暗号データ記憶手段として暗号モードを設定する暗号モード設定手段と、

上記電波検出手段によって上記オフィスに特有の電波が検出されたとき、復号キーを指定する復号キー指定手段と、

この復号キー指定手段によって指定された上記復号キーに従って上記暗号データ記憶手段から上記暗号データを読み出し、これを復号化する復号化手段と、

この復号化手段によって復号化されたデータを上記非暗号データ記憶手段に書き込み、データのアクセス対象を上記非暗号データ記憶手段として非暗号モードを設定する非暗号モード設定手段とを具備したことを特徴とするセキュリティシステム。

【請求項４】　無線環境下でオフィスまたは移動環境で使用されると共に、ネットワークに共有化または非共有化され、非暗号データを記憶するための非暗号データ記憶手段と暗号データを記憶するための暗号データ記憶手段とを有する携帯端末と、

この携帯端末が受信する電波が上記オフィスに特有のものか上記移動環境に特有のものかを検出する電波検出手段と、

この電波検出手段によって上記移動環境に特有の電波が検出されたとき、あるいは、上記携帯端末をネットワークに非共有化するとき、暗号キーを指定する暗号キー指定手段と、

この暗号キー指定手段によって指定された上記暗号キーに従って上記非暗号データ記憶手段から上記非暗号データを読み出し、これを暗号化する暗号化手段と、

この暗号化手段によって暗号化されたデータを上記暗号データ記憶手段に書き込み、データのアクセス対象を上記暗号データ記憶手段として暗号モードを設定する暗号モード設定手段と、

上記電波検出手段によって上記オフィスに特有の電波が検出されたとき、あるいは、上記携帯端末をネットワークに共有化するとき、復号キーを指定する復号キー指定手段と、

この復号キー指定手段によって指定された上記復号キーに従って上記暗号データ記憶手段から上記暗号データを

読み出し、これを復号化する復号化手段と、
この復号化手段によって復号化されたデータを上記非暗号データ記憶手段に書き込み、データのアクセス対象を上記非暗号データ記憶手段として非暗号モードを設定する非暗号モード設定手段とを具備したことを特徴とするセキュリティシステム。
【請求項５】　オフィスまたは移動環境で使用され、非暗号データを記憶するための非暗号データ記憶用メモリと暗号データを記憶するための暗号データ記憶用メモリとを有する携帯端末に対するセキュリティ方法であって、
この携帯端末を上記オフィスから上記移動環境に移動させるとき、暗号キーを指定し、
この指定された上記暗号キーに従って上記非暗号データ記憶用メモリから上記非暗号データを読み出し、これを暗号化した後、
この暗号化されたデータを上記暗号データ記憶用メモリに書き込み、データのアクセス対象を上記暗号データ記憶用メモリとして暗号モードを設定し、
上記携帯端末を上記移動環境から上記オフィスに移動させるとき、復号キーを指定し、
この指定された上記復号キーに従って上記暗号データ記憶用メモリから上記暗号データを読み出し、これを復号化した後、
この暗号化手段によって暗号化されたデータを上記暗号データ記憶用メモリに書き込み、データのアクセス対象を上記非暗号データ記憶用メモリとして非暗号モードを設定するようにしたことを特徴とするセキュリティ方法。
【請求項６】　ネットワークに共有化または非共有化され、非暗号データを記憶するための非暗号データ記憶用メモリと暗号データを記憶するための暗号データ記憶用メモリとを有する携帯端末に対するセキュリティ方法であって、
この携帯端末をネットワークに非共有化するとき、暗号キーを指定し、
この指定された上記暗号キーに従って上記非暗号データ記憶用メモリから上記非暗号データを読み出し、これを暗号化した後、
この暗号化されたデータを上記暗号データ記憶用メモリに書き込み、データのアクセス対象を上記暗号データ記憶用メモリとして暗号モードを設定し、
上記携帯端末をネットワークに共有化するとき、復号キーを指定し、
この指定された上記復号キーに従って上記暗号データ記憶用メモリから上記暗号データを読み出し、これを復号化した後、
この復号化されたデータを上記非暗号データ記憶用メモリに書き込み、データのアクセス対象を上記非暗号データ記憶用メモリとして非暗号モードを設定するようにしたことを特徴とするセキュリティ方法。

【請求項７】　無線環境下でオフィスまたは移動環境で使用され、非暗号データを記憶するための非暗号データ記憶用メモリと暗号データを記憶するための暗号データ記憶用メモリとを有する携帯端末に対するセキュリティ方法であって、
この携帯端末が受信する電波が上記オフィスに特有のものか上記移動環境に特有のものかを検出し、
上記移動環境に特有の電波が検出されたとき、暗号キーを指定し、
この指定された上記暗号キーに従って上記非暗号データ記憶用メモリから上記非暗号データを読み出し、これを暗号化した後、
この暗号化されたデータを上記暗号データ記憶用メモリに書き込み、データのアクセス対象を上記暗号データ記憶用メモリとして暗号モードを設定し、
上記オフィスに特有の電波が検出されたとき、復号キーを指定し、
この指定された上記復号キーに従って上記暗号データ記憶用メモリから上記暗号データを読み出し、これを復号化した後、
この復号化されたデータを上記非暗号データ記憶用メモリに書き込み、データのアクセス対象を上記非暗号データ記憶用メモリとして非暗号モードを設定するようにしたことを特徴とするセキュリティ方法。
【請求項８】　無線環境下でオフィスまたは移動環境で使用されると共に、ネットワークに共有化または非共有化され、非暗号データを記憶するための非暗号データ記憶用メモリと暗号データを記憶するための暗号データ記憶用メモリとを有する携帯端末に対するセキュリティ方法であって、
この携帯端末が受信する電波が上記オフィスに特有のものか上記移動環境に特有のものかを検出し、
上記移動環境に特有の電波が検出されたとき、あるいは、上記携帯端末をネットワークに非共有化するとき、暗号キーを指定し、
この指定された上記暗号キーに従って上記非暗号データ記憶用メモリから上記非暗号データを読み出し、これを暗号化した後、
この暗号化されたデータを上記暗号データ記憶用メモリに書き込み、データのアクセス対象を上記暗号データ記憶用メモリとして暗号モードを設定し、
上記オフィスに特有の電波が検出されたとき、あるいは、上記携帯端末をネットワークに共有化するとき、復号キーを指定し、
この指定された上記復号キーに従って上記暗号データ記憶用メモリから上記暗号データを読み出し、これを復号化した後、
この復号化されたデータを上記非暗号データ記憶用メモリに書き込み、データのアクセス対象を上記非暗号デー

タ記憶用メモリとして非暗号モードを設定するようにしたことを特徴とするセキュリティ方法。

【請求項９】　オフィスまたは移動環境で使用され、非暗号データを記憶するための非暗号データ記憶用メモリと暗号データを記憶するための暗号データ記憶用メモリとを有する携帯端末に対するセキュリティを実現するためのプログラムであって、

この携帯端末を上記オフィスから上記移動環境に移動させるとき、暗号キーを指定し、

この指定された上記暗号キーに従って上記非暗号データ記憶用メモリから上記非暗号データを読み出し、これを暗号化した後、

この暗号化されたデータを上記暗号データ記憶用メモリに書き込み、データのアクセス対象を上記暗号データ記憶用メモリとして暗号モードを設定し、

上記携帯端末を上記移動環境から上記オフィスに移動させるとき、復号キーを指定し、

この指定された上記復号キーに従って上記暗号データ記憶用メモリから上記暗号データを読み出し、これを復号化した後、

この暗号化手段によって暗号化されたデータを上記暗号データ記憶用メモリに書き込み、データのアクセス対象を上記非暗号データ記憶用メモリとして非暗号モードを設定するようにコンピュータを制御するためのプログラムを格納したコンピュータ読取可能な記憶媒体。

【請求項１０】　ネットワークに共有化または非共有化され、非暗号データを記憶するための非暗号データ記憶用メモリと暗号データを記憶するための暗号データ記憶用メモリとを有する携帯端末に対するセキュリティを実現するためのプログラムであって、

この携帯端末をネットワークに非共有化するとき、暗号キーを指定し、

この指定された上記暗号キーに従って上記非暗号データ記憶用メモリから上記非暗号データを読み出し、これを暗号化した後、

この暗号化されたデータを上記暗号データ記憶用メモリに書き込み、データのアクセス対象を上記暗号データ記憶用メモリとして暗号モードを設定し、

上記携帯端末をネットワークに共有化するとき、復号キーを指定し、

この指定された上記復号キーに従って上記暗号データ記憶用メモリから上記暗号データを読み出し、これを復号化した後、

この復号化されたデータを上記非暗号データ記憶用メモリに書き込み、データのアクセス対象を上記非暗号データ記憶用メモリとして非暗号モードを設定するようにコンピュータを制御するためのプログラムを格納したコンピュータ読取可能な記憶媒体。

【請求項１１】　無線環境下でオフィスまたは移動環境で使用され、非暗号データを記憶するための非暗号データ記憶用メモリと暗号データを記憶するための暗号データ記憶用メモリとを有する携帯端末に対するセキュリティを実現するためのプログラムであって、

この携帯端末が受信する電波が上記オフィスに特有のものか上記移動環境に特有のものかを検出し、

上記移動環境に特有の電波が検出されたとき、暗号キーを指定し、

この指定された上記暗号キーに従って上記非暗号データ記憶用メモリから上記非暗号データを読み出し、これを暗号化した後、

この暗号化されたデータを上記暗号データ記憶用メモリに書き込み、データのアクセス対象を上記暗号データ記憶用メモリとして暗号モードを設定し、

上記オフィスに特有の電波が検出されたとき、復号キーを指定し、

この指定された上記復号キーに従って上記暗号データ記憶用メモリから上記暗号データを読み出し、これを復号化した後、

この復号化されたデータを上記非暗号データ記憶用メモリに書き込み、データのアクセス対象を上記非暗号データ記憶用メモリとして非暗号モードを設定するようにコンピュータを制御するためのプログラムを格納したコンピュータ読取可能な記憶媒体。

【請求項１２】　無線環境下でオフィスまたは移動環境で使用されると共に、ネットワークに共有化または非共有化され、非暗号データを記憶するための非暗号データ記憶用メモリと暗号データを記憶するための暗号データ記憶用メモリとを有する携帯端末に対するセキュリティを実現するためのプログラムであって、

この携帯端末が受信する電波が上記オフィスに特有のものか上記移動環境に特有のものかを検出し、

上記移動環境に特有の電波が検出されたとき、あるいは、上記携帯端末をネットワークに非共有化するとき、暗号キーを指定し、

この指定された上記暗号キーに従って上記非暗号データ記憶用メモリから上記非暗号データを読み出し、これを暗号化した後、

この暗号化されたデータを上記暗号データ記憶用メモリに書き込み、データのアクセス対象を上記暗号データ記憶用メモリとして暗号モードを設定し、

上記オフィスに特有の電波が検出されたとき、あるいは、上記携帯端末をネットワークに共有化するとき、復号キーを指定し、

この指定された上記復号キーに従って上記暗号データ記憶用メモリから上記暗号データを読み出し、これを復号化した後、

この復号化されたデータを上記非暗号データ記憶用メモリに書き込み、データのアクセス対象を上記非暗号データ記憶用メモリとして非暗号モードを設定するようにコンピュータを制御するためのプログラムを格納したコンピュータ読取可能な記憶媒体。

ピュータ読取可能な記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、携帯端末で扱うデータのセキュリティを保証するセキュリティシステムに係り、特にオフィスと移動環境とでデータの暗号化／復号化を効率的に行うことでセキュリティを保証するセキュリティシステム及びセキュリティ方法に関する。

【０００２】

【従来の技術】従来、例えばＰＤＡ（personal digital assistants）のような携帯端末にＰＨＳ（personal handyphone system）等の通信機能を備えたものがある。このような携帯端末を持ち歩くことにより、オフィス内はもちろんのこと、オフィス外であってもデータを取り扱うことができる。また、オフィス外であっても、オフィス内に設置されたホストコンピュータ等とデータ通信を行うこともできる。

【０００３】ところで、オフィス外の市街地や、電車などの移動環境にて携帯端末を使用する場合には、置き忘れや盗難などにより携帯端末上のデータが漏洩の危険にさらされるという問題がある。このような問題に対しては、例えばデータの暗号化、携帯端末へのログインによるユーザ認証、ＩＣカードに記録された復号キーを用いた復号化など、種々の方式が実現されている。

【０００４】しかしながら、これらの方式の欠点は携帯端末を使う場所を操作者自ら意識してデータを暗号化しなければならないということである。すなわち、オフィスから移動環境への移動に際しては、オフィス内にある個人専用のパーソナルコンピュータ（ＰＣ）や、グループで共有して使用するサーバコンピュータ上のデータ（ファイル）をその都度暗号化して携帯端末にコピーする、といった作業を忘れずに行う必要がある。

【０００５】なお、常にデータを暗号化するという方法もあるが、一般にオフィス内では暗号化は不要であり、また、そのような暗号化されたデータを使用する場合にはその都度復号化を必要とするため、利便性に欠けるといった問題がある。

【０００６】

【発明が解決しようとする課題】上述したように、従来、携帯端末の置き忘や、盗難などによってデータが漏洩してしまうことを防止するためには、オフィス内にあるコンピュータのデータを取り出す際に、それを暗号化して、携帯端末にコピーするといった作業を行う必要があった。

【０００７】この場合、オフィスと移動環境との間を行き来する場合には、その場所がオフィス内であればデータを暗号化せず、移動環境であればデータを暗号化する、といったように移動場所に応じて適宜暗号化の作業を必要とし、また、暗号化されたデータを復号化する作業も必要となることから、携帯端末を使用する操作者に

負担を掛けると同時に利便性に欠るという問題があった。

【０００８】また、従来では、操作者の判断によってデータの暗号化を適宜行う必要があった。このため、移動環境に移動する際に暗号化を怠る可能性が多々あり、データが漏洩しやすい等の問題があった。

【０００９】本発明は上記のような点に鑑みなされたもので、携帯端末上のデータの暗号化／復号化を簡単に行うことができ、これにより、操作者に負担を掛けることなく、また、利便性に欠くことなくデータを保護することのできるセキュリティシステム及びセキュリティ方法を提供することを目的とする。

【００１０】特に、本発明では、以下のような利便性の高いセキュリティシステム及びセキュリティ方法を提供することを目的とする。

【００１１】（１）オフィスと移動環境間の移動時において、携帯端末上のデータをオフィスでは非暗号データ、移動環境では暗号データに適宜変換可能とする。

【００１２】（２）ネットワーク上で共有化される携帯端末を使用する場合において、携帯端末上のデータを非共有化時には暗号データ、共有化時には非暗号データに適宜変換可能とする。

【００１３】（３）無線環境で携帯端末を使用する場合において、無線電波の種別に応じてオフィス／移動環境を自動的に判断し、携帯端末上のデータをオフィスでは非暗号データ、移動環境では暗号データに適宜変換可能とする。

【００１４】（４）無線環境で使用すると共にネットワーク上で共有化される携帯端末を使用する場合において、携帯端末上のデータをオフィスでは非暗号データ、移動環境では暗号データに適宜変換可能とし、さらに、非共有化時には暗号データ、共有化時には非暗号データに適宜変換可能とする。

【００１５】

【課題を解決するための手段】

（１）本発明のセキュリティシステムは、オフィスまたは移動環境で使用され、非暗号データを記憶するための非暗号データ記憶手段と暗号データを記憶するための暗号データ記憶手段とを有する携帯端末と、この携帯端末を上記オフィスから上記移動環境に移動させるとき、暗号キーを指定する暗号キー指定手段と、この暗号キー指定手段によって指定された上記暗号キーに従って上記非暗号データ記憶手段から上記非暗号データを読み出し、これを暗号化する暗号化手段と、この暗号化手段によって暗号化されたデータを上記暗号データ記憶手段に書き込み、データのアクセス対象を上記暗号データ記憶手段として暗号モードを設定する暗号モード設定手段と、上記携帯端末を上記移動環境から上記オフィスに移動させるとき、復号キーを指定する復号キー指定手段と、この復号キー指定手段によって指定された上記復号キーに従

って上記暗号データ記憶手段から上記暗号データを読み出し、これを復号化する復号化手段と、この復号化手段によって復号化されたデータを上記非暗号データ記憶手段に書き込み、データのアクセス対象を上記非暗号データ記憶手段として非暗号モードを設定する非暗号モード設定手段とを具備したものである。

【００１６】このような構成によれば、携帯端末をオフィスから移動環境に移動させるとき、操作者により指定された暗号キーに従って携帯端末上の非暗号データが暗号化され、その暗号データをアクセス対象とするような暗号モードが設定される。一方、携帯端末を移動環境からオフィスに移動させるとき、操作者により指定された復号キーに従って暗号データが復号化され、その復号データつまり非暗号データをアクセス対象とするような非暗号モードが設定される。

【００１７】このように、オフィスから移動環境に移動するときには、操作者が指定した暗号キーに従って携帯端末上のデータを暗号化して持ち歩くことができる。これにより、移動環境において、盗難や置き忘れなどによってデータが漏洩してしまうのを防ぐことができる。一方、移動環境からオフィスに戻るときには、操作者が指定した暗号キーに従って、その暗号データを復号化して元に戻すことができる。これにより、オフィス内では、常に誰もがデータを確認することができる。

【００１８】（２）また、本発明のセキュリティシステムは、ネットワークに共有化または非共有化され、非暗号データを記憶するための非暗号データ記憶手段と暗号データを記憶するための暗号データ記憶手段とを有する携帯端末と、この携帯端末をネットワークに非共有化するとき、暗号キーを指定する暗号キー指定手段と、この暗号キー指定手段によって指定された上記暗号キーに従って上記非暗号データ記憶手段から上記非暗号データを読み出し、これを暗号化する暗号化手段と、この暗号化手段によって暗号化されたデータを上記暗号データ記憶手段に書き込み、データのアクセス対象を上記暗号データ記憶手段として暗号モードを設定する暗号モード設定手段と、上記携帯端末をネットワークに共有化するとき、復号キーを指定する復号キー指定手段と、この復号キー指定手段によって指定された上記復号キーに従って上記暗号データ記憶手段から上記暗号データを読み出し、これを復号化する復号化手段と、この復号化手段によって復号化されたデータを上記非暗号データ記憶手段に書き込み、データのアクセス対象を上記非暗号データ記憶手段として非暗号モードを設定する非暗号モード設定手段とを具備したものである。

【００１９】このような構成によれば、携帯端末をネットワークに非共有化するとき、操作者により指定された暗号キーに従って携帯端末上の非暗号データが暗号化され、その暗号データをアクセス対象とするような暗号モードが設定される。一方、携帯端末をネットワークに共有化するとき、携帯端末を移動環境からオフィスに移動させるとき、操作者により指定された復号キーに従って暗号データが復号化され、その復号データつまり非暗号データをアクセス対象とするような非暗号モードが設定される。

【００２０】このように、携帯端末上のデータをオフィスに設置されたネットワーク上で共有資源としてＰＣにより共有化している間は暗号データが復号化される。一方、非共有化したときには、データが暗号化されるといった柔軟でかつ安全性の高い携帯端末の利用を実現できる。これにより、移動環境に限らずオフィス内での盗難や起き忘れ時にもデータ保護ができる携帯端末を提供できる。

【００２１】（３）また、本発明のセキュリティシステムは、無線環境下でオフィスまたは移動環境で使用され、非暗号データを記憶するための非暗号データ記憶手段と暗号データを記憶するための暗号データ記憶手段とを有する携帯端末と、この携帯端末が受信する電波が上記オフィスに特有のものか上記移動環境に特有のものかを検出する電波検出手段と、この電波検出手段によって上記移動環境に特有の電波が検出されたとき、暗号キーを指定する暗号キー指定手段と、この暗号キー指定手段によって指定された上記暗号キーに従って上記非暗号データ記憶手段から上記非暗号データを読み出し、これを暗号化する暗号化手段と、この暗号化手段によって暗号化されたデータを上記暗号データ記憶手段に書き込み、データのアクセス対象を上記暗号データ記憶手段として暗号モードを設定する暗号モード設定手段と、上記電波検出手段によって上記オフィスに特有の電波が検出されたとき、復号キーを指定する復号キー指定手段と、この復号キー指定手段によって指定された上記復号キーに従って上記暗号データ記憶手段から上記暗号データを読み出し、これを復号化する復号化手段と、この復号化手段によって復号化されたデータを上記非暗号データ記憶手段に書き込み、データのアクセス対象を上記非暗号データ記憶手段として非暗号モードを設定する非暗号モード設定手段とを具備したものである。

【００２２】このような構成によれば、携帯端末が受信する電波がオフィスに特有のものか移動環境に特有のものかが検出される。移動環境に特有の電波が検出されたとき、操作者により指定された暗号キーに従って携帯端末上の非暗号データが暗号化され、その暗号データをアクセス対象とするような暗号モードが設定される。一方、オフィスに特有の電波が検出されたとき、操作者により指定された復号キーに従って暗号データが復号化され、その復号データつまり非暗号データをアクセス対象とするような非暗号モードが設定される。

【００２３】このように、携帯端末の操作者が自分の存在する環境を意識することなく、電波環境の変化に応じて暗号化／復号化が自動的に行われる。これにより、操

作者が自分の存在する環境では不適切であり、結果として誤った暗号化または復号化の処理を実行するといった操作ミスをなくすことができる。

【００２４】（４）また、本発明のセキュリティシステムは、無線環境下でオフィスまたは移動環境で使用されると共に、ネットワークに共有化または非共有化され、非暗号データを記憶するための非暗号データ記憶手段と暗号データを記憶するための暗号データ記憶手段とを有する携帯端末と、この携帯端末が受信する電波が上記オフィスに特有のものか上記移動環境に特有のものかを検出する電波検出手段と、この電波検出手段によって上記移動環境に特有の電波が検出されたとき、あるいは、上記携帯端末をネットワークに非共有化するとき、暗号キーを指定する暗号キー指定手段と、この暗号キー指定手段によって指定された上記暗号キーに従って上記非暗号データ記憶手段から上記非暗号データを読み出し、これを暗号化する暗号化手段と、この暗号化手段によって暗号化されたデータを上記暗号データ記憶手段に書き込み、データのアクセス対象を上記暗号データ記憶手段として暗号モードを設定する暗号モード設定手段と、上記電波検出手段によって上記オフィスに特有の電波が検出されたとき、あるいは、上記携帯端末をネットワークに共有化するとき、復号キーを指定する復号キー指定手段と、この復号キー指定手段によって指定された上記復号キーに従って上記暗号データ記憶手段から上記暗号データを読み出し、これを復号化する復号化手段と、この復号化手段によって復号化されたデータを上記非暗号データ記憶手段に書き込み、データのアクセス対象を上記非暗号データ記憶手段として非暗号モードを設定する非暗号モード設定手段とを具備したものである。

【００２５】このような構成によれば、移動環境に特有の電波が検出されたとき、あるいは、携帯端末をネットワークに非共有化するとき、操作者により指定された暗号キーに従って携帯端末上の非暗号データが暗号化され、その暗号データをアクセス対象とするような暗号モードが設定される。一方、オフィスに特有の電波が検出されたとき、あるいは、携帯端末をネットワークに共有化するとき、操作者により指定された復号キーに従って暗号データが復号化され、その復号データつまり非暗号データをアクセス対象とするような非暗号モードが設定される。

【００２６】このように、電波環境の変化に応じて暗号化／復号化が行われ、また、携帯端末上のデータをオフィスに設置されたネットワーク上で共有資源としてＰＣにより共有化／非共有化する場合でも暗号化／復号化が行われる。これにより、携帯端末の利便性をさらに向上させることができる。

【００２７】

【発明の実施の形態】以下、図面を参照して本発明の実施形態を説明する。

【００２８】ここでは、第１の実施形態としてオフィスと移動環境間で携帯端末を使用する場合、第２の実施形態としてネットワーク上で携帯端末を共有化／非共有化する場合、第３の実施形態として無線環境で携帯端末を使用する場合をそれぞれ想定したセキュリティシステムについて説明する。

【００２９】（第１の実施形態）図１は本発明の第１の実施形態に係るシステムの全体構成を示すブロック図である。図１に示すように、オフィス１０と移動環境１２を想定する。

【００３０】オフィス１０では、通信機能を備えた携帯端末１０－１ａ、…、１０－１ｎが無線ＬＡＮ基地局１０－２ａと無線ＬＡＮハブ１０－２ｂからなる無線ＬＡＮ１０－２に通信により接続可能であり、さらにＬＡＮ１０－３を介してＰＣ（パーソナルコンピュータ）１０－４ａ、…、１０－４ｎとサーバコンピュータ１０－５にも接続可能である。

【００３１】一方、移動環境１２では、同じく通信機能を備えた携帯端末１２－１ａ、…、１２－１ｎが移動通信網基地局１２－２を介して移動通信網１２－３に通信により接続可能である。ＬＡＮ１０－３と移動通信網１２－３は交換機１１により接続されている。

【００３２】オフィス１０での携帯端末１０－１ａ、…、１０－１ｎと移動環境１２での携帯端末１２－１ａ、…、１２－１ｎは同一のものである。すなわち、オフィス１０と移動環境１２との間を移動しながら携帯端末１０－１ａ、…、１０－１ｎを使用する。以降の説明では携帯端末１０－１ａを用いて説明する。

【００３３】まず、携帯端末１０－１ａの構成を図２を用いて説明する。

【００３４】図２は第１の実施形態における携帯端末１０－１ａの構成を示すブロック図である。図２に示すように、携帯端末１０－１ａは、ＣＰＵ２１、メモリ２２、２次記憶装置２３、ＬＣＤ（Liquid Crystal Display）やＣＲＴ（Cathode Ray Tube）などの画面表示装置２４、キーボードやマウスなどの入力装置２５、無線ＬＡＮ１０－２や移動通信網１２－３との通信を制御する通信制御装置２６から構成される。

【００３５】メモリ２２上には、画面表示を制御する画面制御プログラム２２－１、２次記憶装置２３上の非暗号データを暗号化するための暗号キーを暗号キーレジスタに設定したり、２次記憶装置２３上の暗号データを復号化するための復号キーを復号キーレジスタに設定するキー設定プログラム２２－２、２次記憶装置２３上のデータをアクセスする暗復号化プログラム２２－３、暗復号化プログラム２２－３が２次記憶装置２３上のデータをアクセスするときに使用するデータバッファ２２－４が置かれている。

【００３６】２次記憶装置２３は、例えばＰＣカードのような超小型の記憶装置あるいは磁気ディスクやフラッ

シュメモリなどの不揮発性メモリからなる。この２次記憶装置２３上には、選択回路２３－１、モードレジスタ２３－１ａ、暗号キーレジスタ２３－２、暗号化書込回路２３－３、暗号データ記憶部２３－４、復号キーレジスタ２３－５、復号化読出回路２３－６、書込回路２３－７、非暗号データ記憶部２３－８、読出回路２３－９が置かれている。

【００３７】選択回路２３－１は、キー設定プログラム２２－２からのキー設定要求タイプ（暗号キーか復号キーのどちらかを設定）と暗復号化プログラム２２－３からのアクセス要求タイプ（非暗号データや暗号データの読取りと書込み）を選択する。モードレジスタ２３－１ａは、選択回路２３－１内にあって移動環境１２で非暗号データをアクセスするのか暗号データをアクセスするのかのモードを保持する。

【００３８】暗号キーレジスタ２３－２は、暗号キーを保持する。暗号化書込回路２３－３は、暗復号化プログラム２２－３からのデータを暗号化して暗号データ記憶部２３－４に書込む。暗号データ記憶部２３－４は、暗号化されたデータを記憶する。復号キーレジスタ２３－５は、復号キーを保持する。復号化読出回路２３－６は、暗号データ記憶部２３－４のデータを復号化して読出す。書込回路２３－７は、非暗号データを非暗号データ記憶部２３－８に書込む。非暗号データ記憶部２３－８は、非暗号データを記憶する。読出回路２３－９は、非暗号データ記憶部２３－８のデータを読出す。

【００３９】次に、携帯端末１０－１ａの操作画面を図３を用いて説明する。

【００４０】図３は第１の実施形態における携帯端末１０－１ａの操作画面を示す図である。図３に示すように、携帯端末１０－１ａの操作画面３は、操作者がキー設定プログラム２２－２を用いて暗号キーを暗号キーレジスタ２３－２に設定するための画面３１、暗号データを復号データに戻すときに使用する復号キーをキー設定プログラムにより復号キーレジスタ２３－５に設定するための画面３２、操作者が実際に２次記憶装置２３上の非暗号データまたは暗号データをアクセスするための画面３３の３つから構成される。

【００４１】画面３１では、操作者はパスワード３１－１の入力により正当な操作者であることが認証された後、暗号キー３１－２に暗号キーを指定し、暗号キー設定アイコン３１－３をクリックする。これにより、キー設定プログラム２２－２は暗号キー３１－２に指定された暗号キーを２次記憶装置２３上の暗号キーレジスタ２３－２に格納する。

【００４２】画面３２では、操作者はパスワード３２－１の入力により正当な操作者であることが認証された後、復号キー３２－２に復号キーを指定し、復号キー設定アイコン３２－３をクリックする。これにより、キー設定プログラム２２－２は復号キー３２－２に指定された復号キーを２次記憶装置２３上の復号キーレジスタ２３－５に格納する。

【００４３】画面３３では、操作者がオフィス１０にいる場合と移動環境１２にいる場合とで異なる。すなわち、操作者がオフィス１０にいて移動環境１２に移動するときに選択する暗号化アイコン３３－１と、移動環境１２からオフィス１０に戻ったときに選択する復号化アイコン３３－３と、暗号化または復号化の状況（例えばデータが現在何％暗号化または復号化されているのかを示す完了度合など）を示す状況表示画面３３－２から構成される。

【００４４】ここで、暗号化の場合には、暗号化アイコン３３－１の選択により、暗復号化プログラム２２－３は以下のような一連の暗号化コピー処理を実行することになる。

【００４５】すなわち、読出回路２３－９によりメモリ２２上のデータバッファ２２－４に読み出した非暗号データ記憶部２３－８のデータを暗号化書込回路２３－３により暗号キーレジスタ２３－２内の暗号キーを用いて暗号化し、その暗号化されたデータを暗合号化書込回路２３－３により暗号データ記憶部２３－４に書込む。また、復号化の場合には、復号化アイコン３３－３の選択により、暗復号化プログラム２２－３は以下のような一連の復号化コピー処理を実行することになる。

【００４６】すなわち、暗号データ記憶部２３－４のデータを復号化読出回路２３－６により読み出して復号キーレジスタ２３－５内の復号キーを用いて復号化し、その復号化されたデータ（つまり非暗号データ）を書込回路２３－７により非暗号データ記憶部２３－８に書込む。

【００４７】なお、図３の例では、暗号化の設定画面と復号化の設定画面の一体化された構成を示したが、例えば暗号化時には画面３１と、暗号化アイコン３３－１および状況表示画面３３－２を表示し、暗号化時には画面３２と、復号化アイコン３３－３および状況表示画面３３－２を表示するようにしても良い。

【００４８】次に、図１～図３を前提にしてオフィス１０と移動環境１２との間の移動時におけるデータの暗号化と復号化の処理の流れを説明する。

【００４９】まず、オフィス１０から移動環境１２に移動するときの操作及び処理について図４および図５を用いて説明する。

【００５０】図４および図５は第１の実施形態における暗号化処理の動作を説明するためのフローチャートである。オフィス１０から移動環境１２に移動するとき、操作者が操作画面３１でパスワード３１－１を入力し、正当な操作者であることが認証された後、暗号キー３１－２を入力して暗号キー設定アイコン３１－３をクリックする（ステップＡ１１）。これにより、キー設定プログラム２２－２は２次記憶装置２３上の暗号キーレジスタ

２３－２に暗号キー３１－２を設定する（ステップＡ１２）。

【００５１】操作者が暗号化アイコン３３－１をクリックすると（ステップＡ１３）、暗復号化プログラム２２－３は選択回路２３－１に対して非暗号データ記憶部２３－８上のデータをメモリ２２上のデータバッファ２２－４に読み出すことを指令する（ステップＡ１４）。

【００５２】この暗復号化プログラム２２－３による指令を受けた選択回路２３－１は、読出回路２３－９により非暗号データ記憶部２３－８から非暗号データを読み出し、その非暗号データをメモリ２２上のデータバッファ２２－４に格納する（ステップＡ１５）。

【００５３】次に、暗復号化プログラム２２－３は、データバッファ２２－４上の非暗号データを選択回路２３－１に暗号化して暗号データ記憶部２３－４に格納することを指令する（ステップＡ１６）。

【００５４】この暗復号化プログラム２２－３による指令を受けた選択回路２３－１は、暗号化書込回路２３－３によりデータバッファ２２－４上の非暗号データを暗号キーレジスタ２３－２内の暗号キーを用いて暗号化し、これを暗号データ記憶部２３－４に書込む（ステップＡ１７）。

【００５５】このとき、暗復号化プログラム２２－３は暗号化処理の完了度合（暗号化が何％完了したか）などの状況を画面３３の状況表示画面３３－２に表示する（ステップＡ１８）。

【００５６】以上の読出処理と暗号化書込処理を非暗号データ記憶部２３－８上のデータがなくなるまで繰り返す（ステップＡ１９）。非暗号データ記憶部２３－８上のデータがなくなると（ステップＡ１９のＮｏ）、暗復号化プログラム２２－３は選択回路２３－１内のモードレジスタ２３－１ａを以降の２次記憶装置２３へのアクセスが暗号データ記憶部２３－４に対して行われるように暗号モードに設定し（ステップＡ２０）、暗号化処理完了のメッセージを状況表示画面３３－２に表示する（ステップＡ２１）。

【００５７】次に、移動環境１２からオフィス１０に移動するときの操作及び処理について図６および図７を用いて説明する。

【００５８】図６および図７は第１の実施形態における復号化処理の動作を説明するためのフローチャートである。移動環境１２からオフィス１０に移動するとき、操作者が操作画面３２でパスワード３２－１を入力し、正当な操作者であることが認証された後、復号キー３２－２を入力して復号キー設定アイコン３２－３をクリックする（ステップＢ１１）。これにより。キー設定プログラム２２－２は２次記憶装置２３上の復号キーレジスタ２３－５に復号キー３２－２を設定する（ステップＢ１２）。

【００５９】操作者が復号化アイコン３３－３をクリックすると（ステップＢ１３）、暗復号化プログラム２２－３は選択回路２３－１に対して暗号データ記憶部２３－４上のデータをメモリ２２上のデータバッファ２２－４に読み出すことを指令する（ステップＢ１４）。

【００６０】この暗復号化プログラム２２－３による指令を受けた選択回路２３－１は復号化読出回路２３－６により暗号データ記憶部２３－４から暗号データを読み出して復号キーレジスタ２３－５内の復号キーを用いて復号化し、その復号化されたデータをメモリ２２上のデータバッファ２２－４に格納する（ステップＢ１５）。

【００６１】次に、暗復号化プログラム２２－３はデータバッファ２２－４上の復号化されたデータを選択回路２３－１に対して非暗号データ記憶部２３－８に格納することを指令する（ステップＢ１６）。

【００６２】この暗復号化プログラム２２－３による指令を受けた選択回路２３－１は、書込回路２３－７により非暗号データ記憶部２３－８にデータバッファ２２－４上の非暗号データを書込む（ステップＢ１７）。

【００６３】このとき、暗復号化プログラム２２－３は復号化処理の完了度合（復号化が何％完了したか）などの状況を画面３３の状況表示画面３３－２に表示する（ステップＢ１８）。

【００６４】以上の暗号化読出処理と書込処理を暗号データ記憶部２３－４上のデータがなくなるまで繰り返す（ステップＢ１９）。暗号データ記憶部２３－４上のデータがなくなると（ステップＢ１９のＮｏ）、暗復号化プログラム２２－３は選択回路２３－１内のモードレジスタ２３－１ａを以降の２次記憶装置２３へのアクセスが非暗号データ記憶部２３－８に対して行われるように非暗号モードに設定し（ステップＢ２０）、復号化処理完了のメッセージを状況表示画面３３－２に表示する（ステップＢ２１）。

【００６５】このように、第１の実施形態にあっては、オフィスから移動環境に移動するときには、操作者が指定した暗号キーに従って携帯端末上のデータを暗号化して持ち歩くことができる。つまり、操作者のみが知る暗号キーを用いて暗号化できる。これにより、移動環境において、盗難や置き忘れなどによってデータが漏洩してしまうのを防ぐことができる。一方、移動環境からオフィスに戻るときには、操作者が指定した暗号キーに従って、その暗号データを復号化して元に戻すことができる。これにより、オフィス内では、常に誰もがデータを確認することができる。

【００６６】（第２の実施形態）上述した第１の実施形態では、操作者がプログラムに指示して暗号化あるいは復号化を行っているが、第２の実施形態では、携帯端末のデータをＰＣのデータとしてＬＡＮや無線ＬＡＮを介して共有すること（これをネットワーク共有化と呼ぶ）を復号化実行のトリガーとし、逆に非共有にすること（これをネットワーク非共有化と呼ぶ）を暗号化実行の

トリガーとすることで、前述の操作者の指示の代わりとする。

【００６７】すなわち、通常、オフィスでは、携帯端末を使用せずに高性能で使い易いＰＣを使用するが、この場合に必要なことは携帯端末上のデータをＰＣが処理できるようにネットワーク共有化することである。第２の実施形態では、このことに着目し、オフィスでＰＣが携帯端末上のデータをネットワーク共有化し処理している状況ではデータは復号化し、ＰＣによりネットワーク非共有化されたとき移動環境に携帯端末が移動したものとみなし、それをトリガーとして携帯端末上のデータを暗号化する。

【００６８】以下、図面を参照して本発明の第２の実施形態を説明する。

【００６９】図８は本発明の第２の実施形態に係るシステムの全体構成を示すブロック図である。図８に示すように、オフィス１０ａと移動環境１２ａを想定する。

【００７０】オフィス１０ａでは、通信機能を備えた携帯端末１０ａ－１ａ、…、１０ａ－１ｎが無線ＬＡＮ基地局１０ａ－２ａと無線ＬＡＮハブ１０ａ－２ｂからなる無線ＬＡＮ１０ａ－２と通信により接続可能であり、さらにＬＡＮ１０ａ－３を介してＰＣ（パーソナルコンピュータ）１０ａ－４１、…、１０ａ－４ｎとサーバコンピュータ１０ａ－５にも接続可能である。

【００７１】一方、移動環境１２ａでは、同じく通信機能を備えた携帯端末１２ａ－１ａ、…、１２ａ－１ｎが移動通信網基地局１２ａ－２を介して移動通信網１２ａ－３に通信により接続可能である。ＬＡＮ１０ａ－３と移動通信網１２ａ－３は交換機１１ａにより接続されている。

【００７２】オフィス１０ａでの携帯端末１０ａ－１ａ、…、１０ａ－１ｎと移動環境１２ａでの携帯端末１２ａ－１ａ、…、１２ａ－１ｎは同一のものである。すなわち、オフィス１０ａと移動環境１２ａとの間を移動しながら携帯端末１０ａ－１ａ、…、１０ａ－１ｎを使用する。

【００７３】また、携帯端末１０ａ－１ａ、…１０ａ－１ｎのデータはＰＣ１０ａ－４ａ、…、１０ａ－４ｎによってネットワーク共有化され、ネットワーク共有化時には携帯端末１０ａ－１ａ、…１０ａ－１ｎに内蔵されている２次記憶装置はＰＣ１０ａ－４ａ、…、１０ａ－４ｎの第２の２次記憶装置として機能し、携帯端末１０ａ－１ａ…１０ａ－１ｎの２次記憶装置上のデータはＰＣ１０ａ－４ａ上の別の２次記憶装置上のデータとして共有される。ＰＣ１０ａ－４ａ…、１０ａ－４ｎによってネットワーク非共有化されると、携帯端末１０ａ－１ａ、…１０ａ－１ｎの２次記憶装置としてのみ機能する。

【００７４】さらに１台のＰＣが複数台の携帯端末をネットワーク共有化できるが、以降ではＰＣ１０ａ－４ａが携帯端末１０ａ－１ａ上のデータをネットワーク共有化することを前提として説明する。

【００７５】まず、ＰＣ１０ａ－４ａの構成を図９を用いて説明する。

【００７６】図９は第２の実施形態におけるＰＣ１０ａ－４ａの構成を示すブロック図である。図９に示すように、ＰＣ１０ａ－４ａは、ＣＰＵ２１ａ、メモリ２２ａ、２次記憶装置２３ａ、ＬＣＤ（Liquid Crystal Display）やＣＲＴ（Cathode RayTube）などの画面表示装置２４ａ、キーボードやマウスなどの入力装置２５ａ、ＬＡＮとの通信を制御する通信制御装置２６ａ、ネットワーク共有化された２次記憶装置２７ａから構成される。この２次記憶装置２７ａは、ネットワーク共有化された場合に使用される仮想的な記憶装置である。

【００７７】メモリ２２ａ上には、画面表示を制御する画面制御プログラム２２ａ－１、携帯端末１０ａ－１ａの２次記憶装置上のデータをネットワーク共有化／非共有化するネットワーク共有化プログラム２２ａ－２が置かれている。

【００７８】次に、ＰＣ１０ａ－４ａの操作画面を図１０を用いて説明する。

【００７９】図１０は第２の実施形態における携帯端末１０－１ａの操作画面を示す図である。図１０に示すように、ＰＣ１０ａ－４ａの操作画面３ａは、ネットワーク共有化を設定するための画面３ａ－１、ネットワーク非共有化を設定するための画面３ａ－２、現在共有化されている端末名を表示するための画面３ａ－３から構成される。

【００８０】画面３ａ－１では、ネットワーク共有化するデータを持つ携帯端末１０ａ－１ａの名前３ａ－１ａ、携帯端末１０ａ－１ａの操作者のユーザ識別子３ａ－１ｂ、同操作者のパスワード３ａ－１ｃ、携帯端末１０ａ－１ａの復号化キー３ａ－１ａを入力する。

【００８１】画面３ａ－２では、ネットワーク非共有化するデータを持つ携帯端末１０ａ－１ａの名前３ａ－２ａ、携帯端末１０ａ－１ａの操作者のユーザ識別子３ａ－２ｂ、同操作者のパスワード３ａ－２ｃ、携帯端末１０ａ－１ａの復号化キー３ａ－２ｄを入力する。

【００８２】画面３ａ－３では、現在ネットワーク共有化している携帯端末１０ａ－１ａの名前３ａ－３ａを表示する。

【００８３】次に、携帯端末１０ａ－１ａの構成を図１１を用いて説明する。

【００８４】図１１は第２の実施形態における携帯端末１０ａ－１ａの構成を示すブロック図である。図１１に示すように、携帯端末１０ａ－１ａは、ＣＰＵ４１ａ、メモリ４２ａ、２次記憶装置４３ａ、ＬＣＤ（Liquid Crystal Display）やＣＲＴ（Cathode Ray Tube）などの画面表示装置４４ａ、キーボードやマウスなどの入力装置４５ａ、無線ＬＡＮ１０ａ－２や移動通信網１２ａ－

３との通信を制御する通信制御装置４６ａから構成される。

【００８５】メモリ４２ａ上には、画面表示を制御する画面制御プログラム４２ａ－１、２次記憶装置４３ａ上の非暗号データを暗号化するための暗号キーを暗号キーレジスタに設定したり、２次記憶装置４３ａ上の暗号データを復号化するための復号キーを復号キーレジスタに設定するキー設定プログラム４２ａ－２、２次記憶装置４３ａ上のデータを暗号化したり復号化するためにアクセスする暗復号化プログラム４２ａ－３、暗復号化プログラム４２ａ－３が２次記憶装置４３ａ上のデータをアクセスするときに使用するデータバッファ４２ａ－４が置かれている。さらに、ここでは、ＰＣ１０ａ－４ａによって携帯端末１０ａ－１ａの２次記憶装置４３ａがネットワーク共有化されたとき、あるいは、ネットワーク非共有化されたときにＰＣ１０ａ－４ａが携帯端末１０ａ－１ａに送信する通知メッセージを検出するネットワーク共有化検出プログラム４２ａ－５が置かれている。２次記憶装置４３ａは、例えばＰＣカードのような超小型の記憶装置あるいは磁気ディスクやフラッシュメモリなどの不揮発性メモリからなる。この２次記憶装置４３上には、選択回路４３ａ－１、モードレジスタ４３ａ－１ａ、暗号キーレジスタ４３ａ－２、暗号化書込回路４３ａ－３、暗号データ記憶部４３ａ－４、復号キーレジスタ４３ａ－５、復号化読出回路４３ａ－６、書込回路４３ａ－７、非暗号データ記憶部４３ａ－８、読出回路４３ａ－９が置かれている。

【００８６】選択回路４３ａ－１は、キー設定プログラム４２ａ－２からのキー設定要求タイプ（暗号キーか復号キーのどちらかを設定）と暗復号化プログラム４２ａ－３からのアクセス要求タイプ（非暗号データや暗号データの読取りと書込み）を選択する。モードレジスタ４３ａ－１ａは、選択回路４３ａ－１内にあって移動環境１２ａで非暗号データをアクセスするのか暗号データをアクセスするのかのモードを保持する。

【００８７】暗号キーレジスタ４３ａ－２は、暗号キーを保持する。暗号化書込回路４３ａ－３は、暗復号化プログラム４２ａ－３からのデータを暗号化して暗号データ記憶部４３ａ－４に書込む。暗号データ記憶部４３ａ－４は、暗号化されたデータを記憶する。復号キーレジスタ４３ａ－５は、復号キーを保持する。復号化読出回路４３ａ－６は、暗号データ記憶部４３ａ－４のデータを復号化して読出す。書込回路４３ａ－７は、非暗号データを非暗号データ記憶部４３ａ－８に書込む。非暗号データ記憶部４３ａ－８は、非暗号データを記憶する。読出回路４３ａ－９は、非暗号データ記憶部４３ａ－８のデータを読出す。

【００８８】次に、携帯端末１０ａ－１ａの操作画面を図１２を用いて説明する。

【００８９】図１２は第２の実施形態における携帯端末１０ａ－１ａの操作画面を示す図である。図１２に示すように、携帯端末１０ａ－１ａの操作画面５ａは、ネットワーク共有化時の２次記憶装置４３ａ上のデータの復号化／暗号化の状況を表示するための画面５１ａから構成される。

【００９０】画面５１ａでは、携帯端末１０ａ－１ａの２次記憶装置４３ａ上のデータがＰＣ１０ａ－４ａによってネットワーク非共有化された場合とネットワーク共有化された場合とで異なる。すなわち、ネットワーク非共有時は、暗号化コピー処理を実行する暗復号化プログラム４２ａ－３の実行状況と暗号化完了時のネットワーク共有化ＰＣ１０ａ－４ａの名前表示がなさる。逆に、ネットワーク共有化時は、復号化コピー処理を実行する暗復号化プログラム４２ａ－３の実行状況表示と復号化完了時のネットワーク共有化ＰＣ１０ａ－４ａの名前の消去がなされる。

【００９１】次に、図８～図１１を前提にしてオフィス１０ａと移動環境１２ａとの間の移動時におけるデータの暗号化と復号化の処理の流れを説明する。

【００９２】まず、オフィス１０ａから移動環境１２ａに移動するときの操作及び処理について図６を用いて説明する。

【００９３】図１３および図１４は第２の実施形態におけるネットワーク非共有化処理（暗号化処理）の動作を説明するためのフローチャートである。オフィス１０ａから移動環境１２ａに移動するとき、ＰＣ１０ａ－４ａから携帯端末１０ａ－１ａの２次記憶装置４３ａ上のデータをネットワーク非共有化とする。このため、ＰＣ１０ａ－４ａの操作画面３ａ－２において、操作者がネットワーク非共有化の対象となる携帯端末１０ａ－１ａの名前３ａ－２ａ、携帯端末１０ａ－１ａの操作者のユーザ識別子３ａ－２ｂとパスワード３ａ－２ｃ、携帯端末のデータの暗号キー３ａ－２ｄを入力する（ステップＣ１１）。

【００９４】この入力に従い、ＰＣ１０ａ－４ａのネットワーク共有化プログラム２２ａ－２はネットワーク非共有化実行の通知メッセージをユーザ識別子３ａ－２ｂとパスワード３ａ－２ｃ、暗号キー３ａ－２ｄと共に名前３ａ－２ａに指定された携帯端末１０ａ－１ａに送信する（ステップＣ１２）。

【００９５】この通知メッセージを受信した携帯端末１０ａ－１ａのネットワーク共有化検出プログラム４２ａ－５は、受信したユーザ識別子３ａ－２ｂとパスワード３ａ－２ｃが携帯端末１０ａ－１ａの操作者のものと一致するか否かを検査する（ステップＣ１３）。その結果、正当な操作者であることを認証すると（ステップＣのＹｅｓ）、キー設定プログラム４２ａ－２に制御を移し、キー設定プログラム４２ａ－２は２次記憶装置４３ａ上の暗号キーレジスタ４３ａ－２に通知メッセージ内の暗号キー３ａ－２ｄを設定する（ステップＣ１４）。

【００９６】ここで、暗復号化プログラム４２ａ－３は選択回路４３ａ－１に対して非暗号データ記憶部４３ａ－８上のデータをメモリ４２ａ上のデータバッファ４２ａ－４に読み出すことを指令する（ステップＣ１５）。

【００９７】この暗復号化プログラム４２ａ－３による指令を受けた選択回路４３ａ－１は、読出回路４３ａ－９により非暗号データ記憶部４３ａ－８から非暗号データを読み出し、その非暗号データをメモリ４２ａ上のデータバッファ４２ａ－４に格納する（ステップＣ１６）。

【００９８】次に、暗復号化プログラム４２ａ－３は、データバッファ４２ａ－４上の非暗号データを選択回路４３ａ－１に暗号化して暗号データ記憶部４３ａ－４に格納することを指令する（ステップＣ１７）。

【００９９】この暗復号化プログラム４２ａ－３による指令を受けた選択回路４３ａ－１は、暗号化書込回路４３ａ－３により暗号データ記憶部４３ａ－４にデータバッファ４２ａ－４上の非暗号データを暗号キーレジスタ４３ａ－２内の暗号キーを用いて暗号化し、これを暗号データ記憶部４３ａ－４に書込む（ステップＣ１８）。

【０１００】このとき、暗復号化プログラム４２ａ－３は暗号化処理の完了度合（暗号化が何％完了したか）などの状況を画面５３ａの状況表示画面５３ａ－２に表示する（ステップＣ１９）。

【０１０１】以上の読出処理と暗号化書込処理を非暗号データ記憶部４３ａ－８上のデータがなくなるまで繰り返す（ステップＣ２０）。非暗号データ記憶部４３ａ－８上のデータがなくなると（ステップＣ２０のＮｏ）、暗復号化プログラム４２ａ－３は選択回路４３ａ－１内のモードレジスタ４３ａ－１ａを以降の２次記憶装置へのアクセスが暗号データ記憶部４３ａ－８に対して行われるように暗号モードに設定する（ステップＣ２１）。

【０１０２】また、暗復号化プログラム４２ａ－３は暗号化処理完了のメッセージをＰＣ１０ａ－４ａに通知すると共に、その暗号化処理完了のメッセージを状況表示画面５１ａに表示して、これまで表示されていたネットワーク共有化ＰＣ１０ａ－４ａの名前を消去する（ステップＣ２２）。

【０１０３】一方、上記ステップＣ１３において、ネットワーク共有化検出プログラム４２ａ－５が不当な操作者であることを検出した場合には（ステップＣ１３のＮｏ）、エラーメッセージをＰＣ１０ａ－４ａに返信すると共に、そのエラーメッセージを状況表示画面に表示して、直ちにデータの暗号化を中止する（ステップＣ２３）。

【０１０４】次に、移動環境１２ａからオフィス１０ａに移動するときの操作及び処理について図１５および図１６を用いて説明する。

【０１０５】図１５および図１６は第２の実施形態におけるネットワーク共有化処理（復号化処理）の動作を説明するためのフローチャートである。移動環境１２ａからオフィス１０ａに移動するとき、ＰＣ１０ａ－４ａから携帯端末１０ａ－１ａの２次記憶装置４３ａ上のデータをネットワーク共有化とする。このため、ＰＣ１０ａ－４ａの操作画面３ａ－１において、操作者がネットワーク共有化の対象となる携帯端末１０ａ－１ａの名前３ａ－１ａ、携帯端末１０ａ－１ａの操作者のユーザ識別子３ａ－１ｂとパスワード３ａ－１ｃ、携帯端末のデータの復号キー３ａ－１ｄを入力する（ステップＤ１１）。

【０１０６】この入力に従い、ＰＣ１０ａ－４ａのネットワーク共有化プログラム２２ａ－２はネットワーク共有化実行の通知メッセージをユーザ識別子３ａ－１ｂとパスワード３ａ－１ｃ、復号キー３ａ－１ｄと共に名前３ａ－１ａに指定された携帯端末１０ａ－１ａに送信する（ステップＤ１２）。

【０１０７】この通知メッセージを受信した携帯端末１０ａ－１ａのネットワーク共有化検出プログラム４２ａ－５は、受信したユーザ識別子３ａ－１ｂとパスワード３ａ－１ｃが携帯端末１０ａ－１ａの操作者のものと一致するか否かを検査する（ステップＤ１３）。その結果、正当な操作者であることを認証すると（ステップＤ１３のＹｅｓ）、キー設定プログラム４２ａ－２に制御を移し、キー設定プログラム４２ａ－２は２次記憶装置４３ａ上の復号キーレジスタ４３ａ－５に通知メッセージ内の復号キー３ａ－１ｄを設定する（ステップＤ１４）。

【０１０８】ここで、暗復号化プログラム４２ａ－３は選択回路４３ａ－１に対して暗号データ記憶部４３ａ－４上のデータをメモリ４２ａ上のデータバッファ４２ａ－４に読み出すことを指令する（ステップＤ１５）。

【０１０９】この暗復号化プログラム４２ａ－３による指令を受けた選択回路４３ａ－１は、復号化読出回路４３ａ－６により暗号データ記憶部４３ａ－４から暗号データを読み出して復号キーレジスタ４３ａ－５内の復号キーを用いて復号化し、その復号化されたデータをメモリ４２ａ上のデータバッファ４２ａ－４に格納する（ステップＤ１６）。

【０１１０】次に、暗復号化プログラム４２ａ－３は、データバッファ４２ａ－４上の復号化されたデータを選択回路４３ａ－１に対して非暗号データ記憶部４３ａ－８に格納することを指令する（ステップＤ１７）。

【０１１１】この暗復号化プログラム４２ａ－３による指令を受けた選択回路４３ａ－１は、書込回路４３ａ－７により非暗号データ記憶部４３ａ－８にデータバッファ４２ａ－４上の非暗号データを書込む（ステップＤ１８）。

【０１１２】このとき、暗復号化プログラム４２ａ－３は復号化処理の完了度合（復号化が何％完了したか）などの状況を画面５３ａの状況表示画面５３ａ－２に表示

する（ステップＤ１９）。

【０１１３】以上の暗号化読出処理と書込処理を暗号データ記憶部４３ａ－４上のデータがなくなるまで繰り返す（ステップＤ２０）。暗号データ記憶部４３ａ－４上のデータがなくなると（ステップＤ２０のＮｏ）、暗復号化プログラム４２ａ－３は選択回路４３ａ－１内のモードレジスタ４３ａ－１ａを以降の２次記憶装置へのアクセスが非暗号データ記憶部４３ａ－８に対して行われるように非暗号モードに設定する（ステップＤ２１）。

【０１１４】また、暗復号化プログラム４２ａ－３は復号化処理完了のメッセージをＰＣ１０ａ－４ａに通知すると共に、その復号化処理完了のメッセージを状況表示画面５３ａ－２に表示して、ネットワーク共有化ＰＣ１０ａ－４ａの名前を表示する（ステップＤ２２）。

【０１１５】一方、上記ステップＤ１３において、ネットワーク共有化検出プログラム４２ａ－５が不当な操作者であることを検出すると（ステップＤ１３のＮｏ）、エラーメッセージをＰＣ１０ａ－４ａに返信すると共に、そのエラーメッセージを状況表示画面に表示して、直ちにデータの復号化を中止する（ステップＤ２３）。このように、第２の実施形態にあっては、携帯端末上のデータをオフィスに設置されたネットワーク上で共有資源としてＰＣにより共有化（ＰＣに論理的に取り付けることと同義）している間は暗号データが復号化される。一方、非共有化（ＰＣから論理的に取り外すことと同義）したときには、データが暗号化されるといった柔軟でかつ安全性の高い携帯端末の利用を実現できる。これにより、移動環境に限らずオフィス内での盗難や起き忘れ時にもデータ保護ができる携帯端末を提供できる。

【０１１６】（第３の実施形態）上述した第１の実施形態では、操作者がプログラムに指示して暗号化あるいは復号化を行っているが、第３の実施形態では、携帯端末が電波の強度と種別を検出することにより、操作者が自分の存在する環境を認識して暗号化か復号化かを指定するのではなく、その環境で最強の電波がオフィス内で使用されている無線ＬＡＮなのかあるいは移動通信環境で使用されている移動通信網なのかを自動的に判断する。そして、最強の電波が無線ＬＡＮの規格のものであれば携帯端末のデータを復号化し、移動通信網の規格のものであれば暗号化することにより、利便性の高い携帯端末を提供する。

【０１１７】以下、図面を参照して本発明の第３の実施形態を説明する。

【０１１８】図１７は本発明の第３の実施形態に係るシステムの全体構成を示すブロック図である。図１７に示すように、オフィス１０ｂと移動環境１２ｂを想定する。

【０１１９】オフィス１０ｂでは、通信機能を備えた携帯端末１０ｂ－１ａ、…、１０ｂ－１ｎが無線ＬＡＮ基地局１０ｂ－２ａと無線ＬＡＮハブ１０ｂ－２ｂからなる無線ＬＡＮ１０ｂ－２と通信により接続可能であり、さらにＬＡＮ１０ｂ－３を介してＰＣ（パーソナルコンピュータ）１０ｂ－４ａ、…、１０ｂ－４ｎとサーバコンピュータ１０ｂ－５にも接続可能である。

【０１２０】一方、移動環境１２ｂでは、同じく通信機能を備えた携帯端末１２ｂ－１ａ、…、１２ｂ－１ｎが移動通信網基地局１２ｂ－２を介して移動通信網１２ｂ－３に通信により接続可能である。ＬＡＮ１０ｂ－３と移動通信網１２ｂ－３は交換機１１ｂにより接続されている。

【０１２１】オフィス１０ｂでの携帯端末１０ｂ－１ａ、…、１０ｂ－１ｎと移動環境１２ｂでの携帯端末１２ｂ－１ａ、…、１２－１ｎは同一のものである。すなわち、オフィス１０ｂと移動環境１２ｂとの間を移動しながら携帯端末１０ｂ－１ａ、…、１０ｂ－１ｎを使用する。以降の説明では携帯端末１０ｂ－１ａを用いて説明する。

【０１２２】まず、携帯端末１０ｂ－１ａの構成を図１８を用いて説明する。

【０１２３】図１８は第３の実施形態における携帯端末１０ｂ－１ａの構成を示すブロック図である。図１８に示すように、携帯端末１０ｂ－１ａは、ＣＰＵ２１ｂ、メモリ２２ｂ－２次記憶装置２３ｂ、ＬＣＤ（Liquid Crystal Display）やＣＲＴ（Cathode Ray Tube）などの画面表示装置２４ｂ、キーボードやマウスなどの入力装置２５ｂ、無線ＬＡＮ１０ｂ－２や移動通信網１２ｂ－３との通信を制御する通信制御装置２６ｂ、無線ＬＡＮ１０ｂ－２や移動通信網１２ｂ－３の電波の強度や種別を検出する電波検出装置２７ｂから構成される。

【０１２４】メモリ２２ｂ上には、画面表示を制御する画面制御プログラム２２ｂ－１、２次記憶装置２３ｂ上の非暗号データを暗号化するための暗号キーを暗号キーレジスタに設定したり、２次記憶装置２３ｂ上の暗号データを復号化するための復号キーを復号キーレジスタに設定するキー設定プログラム２２ｂ－２、２次記憶装置２３ｂ上の暗号データか非暗号データのどちらをアクセスするのかの設定を行うモード設定プログラム２２ｂ－３が置かれている。

【０１２５】２次記憶装置２３ｂは、例えばＰＣカードのような超小型の記憶装置あるいは磁気ディスクやフラッシュメモリなどの不揮発性メモリからなる。この２次記憶装置２３ｂ上には、選択回路２３ｂ－１、モードレジスタ２３ｂ－１ａ、暗号キーレジスタ２３ｂ－２、暗号化書込回路２３ｂ－３、暗号データ記憶部２３ｂ－４、復号キーレジスタ２３ｂ－５、復号化読出回路２３ｂ－６、書込回路２３ｂ－７、非暗号データ記憶部２３ｂ－８、読出回路２３ｂ－９が置かれている。

【０１２６】選択回路２３ｂ－１は、キー設定プログラム２２－２からのキー設定要求タイプ（暗号キーか復号キーのどちらかを設定）と暗復号化プログラム２２－３

からのアクセス要求タイプ（非暗号データや暗号データの読取りと書込み）を選択する。モードレジスタ２３ｂ－１ａは、選択回路２３ｂ－１内にあって移動環境１２ｂで非暗号データをアクセスするのか暗号データをアクセスするのかのモードを保持する。

【０１２７】暗号キーレジスタ２３ｂ－２は、暗号キーを保持する。暗号化書込回路２３ｂ－３は、暗復号化プログラム２２－３からのデータを暗号化して暗号データ記憶部２３ｂ－４に書込む。暗号データ記憶部２３ｂ－４は、暗号化されたデータを記憶する。復号キーレジスタ２３ｂ－５は、復号キーを保持する。復号化読出回路２３ｂ－６は、暗号データ記憶部２３ｂ－４のデータを復号化して読出す。書込回路２３ｂ－７は、非暗号データを非暗号データ記憶部２３ｂ－８に書込む。非暗号データ記憶部２３ｂ－８は、非暗号データを記憶する。読出回路２３ｂ－９は、非暗号データ記憶部２３ｂ－８のデータを読出す。

【０１２８】次に、携帯端末１０ｂ－１ａの操作画面を図１９を用いて説明する。

【０１２９】図１９は第３の実施形態における携帯端末１０ｂ－１ａの操作画面を示す図である。図１９に示すように、携帯端末１０ｂ－１ａの操作画面３ｂは、操作者がキー設定プログラム２２ｂ－２を用いて暗号キーを暗号キーレジスタ２３ｂ－２に設定するための画面３１ｂ、暗号データを復号データに戻すときに使用する復号キーをキー設定プログラムにより復号キーレジスタ２３ｂ－５に設定するための画面３２ｂ、操作者が実際に２次記憶装置２３ｂ上の非暗号データまたは暗号データをアクセスするための画面３３ｂの３つから構成される。

【０１３０】電波検出プログラム２２ｂ－４が電波検出装置２７ｂを通じて検出した最強の電波が移動環境１２ｂで利用されている移動通信網の規格の電波であれば、画面３１ｂを表示して操作者に暗号手続きを促す。これに対し、操作者はパスワード３１ｂ－１を入力して正当な操作者であることが認証された後、暗号キー３１ｂ－２に暗号キーを指定して暗号キー設定アイコン３１ｂ－３をクリックする。これにより、キー設定プログラム２２ｂ－２は暗号キー３１ｂ－２に指定された暗号キーを２次記憶装置２３ｂ上の暗号キーレジスタ２３ｂ－２に設定する。

【０１３１】また、電波検出プログラム２２ｂ－４の検出した電波が無線ＬＡＮの電波であれば、画面３２ｂを表示して操作者に復号化の手続きを促す。これに対し、操作者はパスワード３２ｂ－１を入力して正当な操作者であることが認証された後、復号キー３２ｂ－２に復号キーを指定し、復号キー設定アイコン３２ｂ－３をクリックする。これにより、キー設定プログラム２２ｂ－２は復号キー３２ｂ－２に指定された復号キーを２次記憶装置２３ｂ上の復号キーレジスタ２３ｂ－５に設定する。

【０１３２】画面３３ｂは、暗復号化プログラム２２ｂ－３の実行の状況表示画面であり、暗号化または復号化の状況（例えばデータが現在何％暗号化または復号化されているのかを示す完了度合など）を示す。

【０１３３】次に、図１７～図１９を前提にしてオフィス１０ｂと移動環境１２ｂとの間の移動時におけるデータの暗号化と復号化の処理の流れを説明する。

【０１３４】まず、電波検出とその種別分析に基づく暗号化あるいは復号化処理の実行について図２０を用いて説明する。

【０１３５】図２０は第３の実施形態における電波種別に応じた暗号化／復号化の判断処理の動作を説明するためのフローチャートである。携帯端末１０ｂ－１ａの存在する環境がオフィス１０ｂか移動環境１２ｂかを電波検出プログラム２２ｂ－４が電波検出装置２７ｂを利用して検出分析する（ステップＥ１１）。その際に、前回の検出時の電波種別と同じか否かを検査し（ステップＥ１２）、異なっている場合には（ステップＥ１２のＮｏ）。電波がどの規格かを検査する（ステップＥ１３）。

【０１３６】ここで、移動環境１２ｂにおける移動通信網１２ｂ－３の規格の電波であれば、後述する図２１および図２２に示す暗号化処理のサブルーチンを呼び出す（ステップＥ１４）。一方、オフィス１０ｂにおける無線ＬＡＮ１０ｂ－２の電波であれば、後述する図２３および図２４に示す復号化処理のサブルーチンを呼び出す（ステップＥ１５）。制御が戻されたら、あるいはステップＥ１２で前回と同一電波であれば、ここでの処理を終了する。

【０１３７】なお、移動通信網の電波としては、携帯電話で１．５ＧＨｚ、ＰＨＳで１．９ＧＨｚが使用されている。これに対し、無線ＬＡＮの電波としては、２．４ＧＨｚと１９ＧＨｚが使用されている。

【０１３８】次に、暗号化処理について図２１および図２２を用いて説明する。

【０１３９】図２１および図２２は第３の実施形態における暗号化処理の動作を説明するためのフローチャートである。受信電波の種類が移動環境１２ｂにおける移動通信網１２ｂ－３の規格の電波であったとき、操作者が操作画面３１ｂでパスワード３１ｂ－１を入力し、正当な操作者であることが認証された後、暗号キー３１－２を入力して暗号キー設定アイコン３１ｂ－３をクリックする（ステップＦ１１）。これにより、キー設定プログラム２２ｂ－２は２次記憶装置２３ｂ上の暗号キーレジスタ２３ｂ－２に暗号キー３１ｂ－２を設定する（ステップＦ１２）。操作者が暗号化アイコン３３ｂ－１をクリックすると（ステップＦ１３）、暗復号化プログラム２２ｂ－３は選択回路２３ｂ－１に対して非暗号データ記憶部２３ｂ－８上のデータをメモリ２２ｂ上のデータバッファ２２ｂ－４に読み出すことを指令する（ステッ

プＦ１４）。

【０１４０】この暗復号化プログラム２２ｂ－３による指令を受けた選択回路２３ｂ－１は読出回路２３ｂ－９により非暗号データ記憶部２３ｂ－８から非暗号データを読み出し、その非暗号データをメモリ２２ｂ上のデータバッファ２２ｂ－４に格納する（ステップＦ１５）。

【０１４１】次に、暗復号化プログラム２２ｂ－３は、データバッファ２２ｂ－４上の非暗号データを選択回路２３ｂ－１に暗号化して暗号データ記憶部２３ｂ－４に格納することを指令する（ステップＦ１６）。

【０１４２】この暗復号化プログラム２２ｂ－３による指令を受けた選択回路２３ｂ－１は、暗号化書込回路２３ｂ－３によりデータバッファ２２ｂ－４上の非暗号データを暗号キーレジスタ２３ｂ－２内の暗号キーを用いて暗号化し、これを暗号データ記憶部２３ｂ－４に書込む（ステップＦ１７）。

【０１４３】このとき、暗復号化プログラム２２ｂ－３は暗号化処理の完了度合（暗号化が何％完了したか）などの状況を画面３３の状況表示画面３３ｂ－２に表示する（ステップＦ１８）。

【０１４４】以上の読出処理と暗号化書込処理を非暗号データ記憶部２３ｂ－８上のデータがなくなるまで繰り返す（ステップＦ１９）。非暗号データ記憶部２３ｂ－８上のデータがなくなると（ステップＦ１９のＮｏ）、暗復号化プログラム２２ｂ－３は選択回路２３ｂ－１内のモードレジスタ２３ｂ－１ａを以降の２次記憶装置２３ｂへのアクセスが暗号データ記憶部２３ｂ－４に対して行われるように暗号モードに設定し（ステップＦ２０）、暗号化処理完了のメッセージを状況表示画面３３ｂ－２に表示する（ステップＦ２１）。

【０１４５】次に、復号化処理について図２３および図２４を用いて説明する。

【０１４６】図２３および図２４は第３の実施形態における復号化処理の動作を説明するためのフローチャートである。受信電波の種類がオフィス１０ｂにおける無線ＬＡＮ１０ｂ－２の電波であったとき、操作者が操作画面３２ｂでパスワード３２ｂ－１を入力し、正当な操作者であることが認証された後、復号キー３２ｂ－２を入力して復号キー設定アイコン３２ｂ－３をクリックする（ステップＧ１１）。これにより、キー設定プログラム２２ｂ－２は２次記憶装置２３ｂ上の復号キーレジスタ２３ｂ－５に復号キー３２ｂ－２を設定する（ステップＧ１２）。

【０１４７】操作者が復号化アイコン３３ｂ－３をクリックすると（ステップＧ１３）、暗復号化プログラム２２ｂ－３は選択回路２３ｂ－１に対して暗号データ記憶部２３ｂ－４上のデータをメモリ２２ｂ上のデータバッファ２２ｂ－４に読み出すことを指令する（ステップＧ１４）。

【０１４８】この暗復号化プログラム２２ｂ－３による指令を受けた選択回路２３ｂ－１は復号化読出回路２３ｂ－６により暗号データ記憶部２３ｂ－４から暗号データを読み出して復号キーレジスタ２３ｂ－５内の復号キーを用いて復号化し、その復号化されたデータをメモリ２２ｂ上のデータバッファ２２ｂ－４に格納する（ステップＧ１５）。

【０１４９】次に、暗復号化プログラム２２ｂ－３は、データバッファ２２ｂ－４上の復号化されたデータを選択回路２３ｂ－１に対して非暗号データ記憶部２３ｂ－８に格納することを指令する（ステップＧ１６）。

【０１５０】この暗復号化プログラム２２ｂ－３による指令を受けた選択回路２３ｂ－１は、書込回路２３ｂ－７により非暗号データ記憶部２３ｂ－８にデータバッファ２２ｂ－４上の非暗号データを書込む（ステップＧ１７）。

【０１５１】このとき、復号化処理の完了度合（復号化が何％完了したか）などの状況を暗復号化プログラム２２ｂ－３は画面３３ｂの状況表示画面３３ｂ－２に表示する（ステップＧ１８）。

【０１５２】以上の暗号化読出処理と書込処理を暗号データ記憶部２３ｂ－４上のデータがなくなるまで繰り返す（ステップＧ１９）。暗号データ記憶部２３ｂ－４上のデータがなくなると（ステップＧ１９のＮｏ）、暗復号化プログラム２２ｂ－３は選択回路２３ｂ－１内のモードレジスタ２３ｂ－１ａを以降の２次記憶装置２３ｂへのアクセスが非暗号データ記憶部２３ｂ－８に対して行われるように非暗号モードに設定し（ステップＧ２０）、復号化処理完了のメッセージを状況表示画面３３ｂ－２に表示する（ステップＧ２１）。

【０１５３】以上の暗号化処理と復号化処理は、電波環境の変化を常時チェックしておき、その変化を捕らえた時点でのみ実行される。例えば無線ＬＡＮから移動通信網へ、あるいはこの逆といった場合で最初に電波の環境が切り換わった時点に実行される。このチェックは電波検出プログラム２２ｂ－４が行う。

【０１５４】このように、第３の実施形態にあっては、携帯端末の操作者が自分の存在する環境を意識することなく、電波環境の変化に応じて暗号化／復号化が自動的に行われる。これにより、操作者が自分の存在する環境では不適切であり、結果として誤った暗号化または復号化の処理を実行するといった操作ミスをなくすことができる。

【０１５５】なお、この第３の実施形態に上記第２の実施形態に適用することも可能である。この場合、携帯端末はオフィスまたは移動環境で使用されると共に、その携帯端末はネットワークに共有化または非共有化される。このような環境下において、移動環境に特有の電波が検出されたとき、あるいは、携帯端末をネットワークに非共有化するときには、操作者が指定した暗号キーに従って暗号化処理を行う。また、オフィスに特有の電波

が検出されたとき、あるいは、携帯端末をネットワークに共有化するときには、操作者が指定した復号キーに従って復号化処理を行う。

【０１５６】このように、電波環境の変化に応じて暗号化／復号化を行い、また、携帯端末上のデータをオフィスに設置されたネットワーク上で共有資源としてＰＣにより共有化／非共有化する場合に暗号化／復号化を行う構成とすることにより、利便性をさらに向上させることができる。

【０１５７】なお、上述した各実施形態において記載した手法は、コンピュータに実行させることのできるプログラムとして、例えば磁気ディスク（フロッピーディスク、ハードディスク等）、光ディスク（ＣＤ－ＲＯＭ、ＤＶＤ等）、半導体メモリなどの記憶媒体に書き込んで各種装置に適用したり、さらに通信媒体により伝送して各種装置に適用することも可能である。本システムを実現するコンピュータは、記録媒体に記録されたプログラムを読み込み、このプログラムによって動作が制御されることにより、上述した処理を実行する。

【０１５８】

【発明の効果】以上のように本発明によれば、携帯端末上のデータの暗号化／復号化を簡単に行うことができ、これにより、操作者に負担を掛けることなく、また、利便性に欠くことなくデータを保護することができる。

【０１５９】特に、携帯端末をオフィスから移動環境に移動させるとき、操作者により指定された暗号キーに従って携帯端末上の非暗号データを暗号化し、その暗号データをアクセス対象とするような暗号モードを設定し、携帯端末を移動環境からオフィスに移動させるとき、操作者により指定された復号キーに従って暗号データを復号化し、その復号データつまり非暗号データをアクセス対象とするような非暗号モードを設定するようにしたため、以下のような効果が得られる。

【０１６０】オフィスから移動環境に移動するときには、操作者が指定した暗号キーに従って携帯端末上のデータを暗号化して持ち歩くことができる。これにより、移動環境において、盗難や置き忘れなどによってデータが漏洩してしまうのを防ぐことができる。一方、移動環境からオフィスに戻るときには、操作者が指定した暗号キーに従って、その暗号データを復号化して元に戻すことができる。これにより、オフィス内では、常に誰もがデータを確認することができる。

【０１６１】また、携帯端末をネットワークに非共有化するとき、操作者により指定された暗号キーに従って携帯端末上の非暗号データを暗号化し、その暗号データをアクセス対象とするような暗号モードを設定し、携帯端末をネットワークに共有化するとき、携帯端末を移動環境からオフィスに移動させるとき、操作者により指定された復号キーに従って暗号データを復号化し、その復号データつまり非暗号データをアクセス対象とするような非暗号モードを設定するようにしたため、以下のような効果が得られる。

【０１６２】携帯端末上のデータをオフィスに設置されたネットワーク上で共有資源としてＰＣにより共有化している間は暗号データが復号化される。一方、非共有化したときには、データが暗号化されるといった柔軟でかつ安全性の高い携帯端末の利用を実現できる。これにより、移動環境に限らずオフィス内での盗難や起き忘れ時にもデータ保護ができる携帯端末を提供できる。

【０１６３】また、携帯端末が受信する電波がオフィスに特有のものか移動環境に特有のものかを検出し、移動環境に特有の電波であれば、操作者により指定された暗号キーに従って携帯端末上の非暗号データを暗号化し、その暗号データをアクセス対象とするような暗号モードを設定し、オフィスに特有の電波であれば、操作者により指定された復号キーに従って暗号データを復号化し、その復号データつまり非暗号データをアクセス対象とするような非暗号モードを設定するようにしたため、以下のような効果が得られる。

【０１６４】携帯端末の操作者が自分の存在する環境を意識することなく、電波環境の変化に応じて暗号化／復号化が自動的に行われる。これにより、操作者が自分の存在する環境では不適切であり、結果として誤った暗号化または復号化の処理を実行するといった操作ミスをなくすことができる。

【０１６５】また、移動環境に特有の電波を検出したとき、あるいは、携帯端末をネットワークに非共有化するとき、操作者により指定された暗号キーに従って携帯端末上の非暗号データを暗号化し、その暗号データをアクセス対象とするような暗号モードを設定し、オフィスに特有の電波を検出したとき、あるいは、携帯端末をネットワークに共有化するとき、操作者により指定された復号キーに従って暗号データを復号化し、その復号データつまり非暗号データをアクセス対象とするような非暗号モードを設定するようにしたため、以下のような効果が得られる。

【０１６６】電波環境の変化に応じて暗号化／復号化が行われ、また、携帯端末上のデータをオフィスに設置されたネットワーク上で共有資源としてＰＣにより共有化／非共有化する場合でも暗号化／復号化が行われる。これにより、携帯端末の利便性をさらに向上させることができる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態に係るシステムの全体構成を示すブロック図。

【図２】第１の実施形態における携帯端末の構成を示すブロック図。

【図３】第１の実施形態における携帯端末の操作画面を示す図。

【図４】第１の実施形態における暗号化処理の動作を説

明するためのフローチャート。

【図５】第１の実施形態における暗号化処理の動作を説明するためのフローチャート。

【図６】第１の実施形態における復号化処理の動作を説明するためのフローチャート。

【図７】第１の実施形態における復号化処理の動作を説明するためのフローチャート。

【図８】本発明の第２の実施形態に係るシステムの全体構成を示すブロック図。

【図９】第２の実施形態におけるＰＣの構成を示すブロック図。

【図１０】第２の実施形態における携帯端末の操作画面を示す図。

【図１１】第２の実施形態における携帯端末の構成を示すブロック図。

【図１２】第２の実施形態における携帯端末の操作画面を示す図。

【図１３】第２の実施形態におけるネットワーク非共有化処理（暗号化処理）の動作を説明するためのフローチャート。

【図１４】第２の実施形態におけるネットワーク非共有化処理（暗号化処理）の動作を説明するためのフローチャート。

【図１５】第２の実施形態におけるネットワーク共有化処理（復号化処理）の動作を説明するためのフローチャート。

【図１６】第２の実施形態におけるネットワーク共有化処理（復号化処理）の動作を説明するためのフローチャート。

【図１７】本発明の第３の実施形態に係るシステムの全体構成を示すブロック図。

【図１８】第３の実施形態における携帯端末の構成を示すブロック図。

【図１９】第３の実施形態における携帯端末の操作画面を示す図。

【図２０】第３の実施形態における電波種別に応じた暗

号化／復号化の判断処理の動作を説明するためのフローチャート。

【図２１】第３の実施形態における暗号化処理の動作を説明するためのフローチャート。

【図２２】第３の実施形態における暗号化処理の動作を説明するためのフローチャート。

【図２３】第３の実施形態における復号化処理の動作を説明するためのフローチャート。

【図２４】第３の実施形態における復号化処理の動作を説明するためのフローチャート。

【符号の説明】

１０…オフィス

１０－１ａ，１０－１ｎ…携帯端末

１０－２…無線ＬＡＮ

１０－３…ＬＡＮ

１０－４ａ，１０－４ｎ…ＰＣ

１０－５…サーバコンピュータ

１１…交換機

１２…移動環境

１２－１ａ，１２－１ｎ…携帯端末

１２－２…移動通信網基地局

１２－３…移動通信網

２１…ＣＰＵ

２２…メモリ

２３…２次記憶装置

２３－１…選択回路

２３－１ａ…モードレジスタ

２３－２…暗号キーレジスタ

２３－３…暗号化書込回路

２３－４…暗号データ記憶部

２３－５…復号キーレジスタ

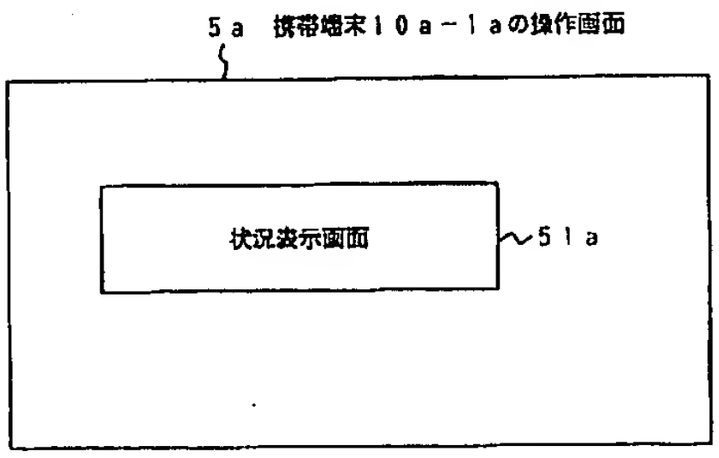
２３－６…復号化読出回路

２３－７…書込回路

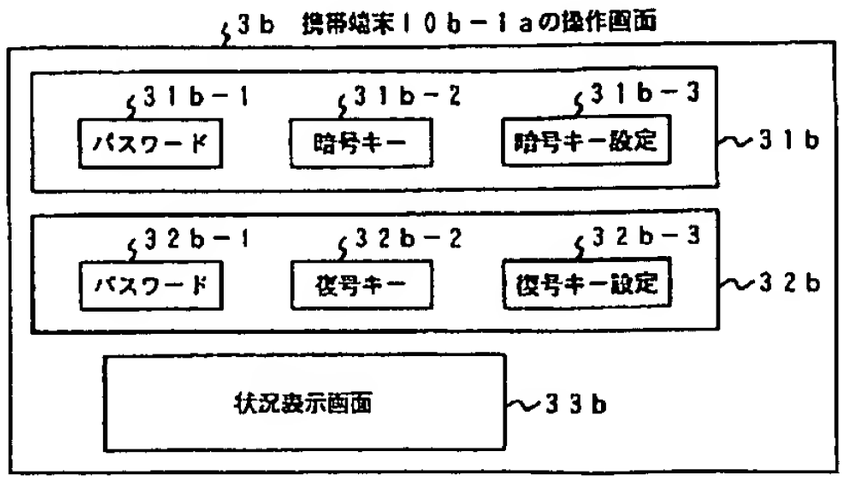
２３－８…非暗号データ記憶部

２３－９…読出回路

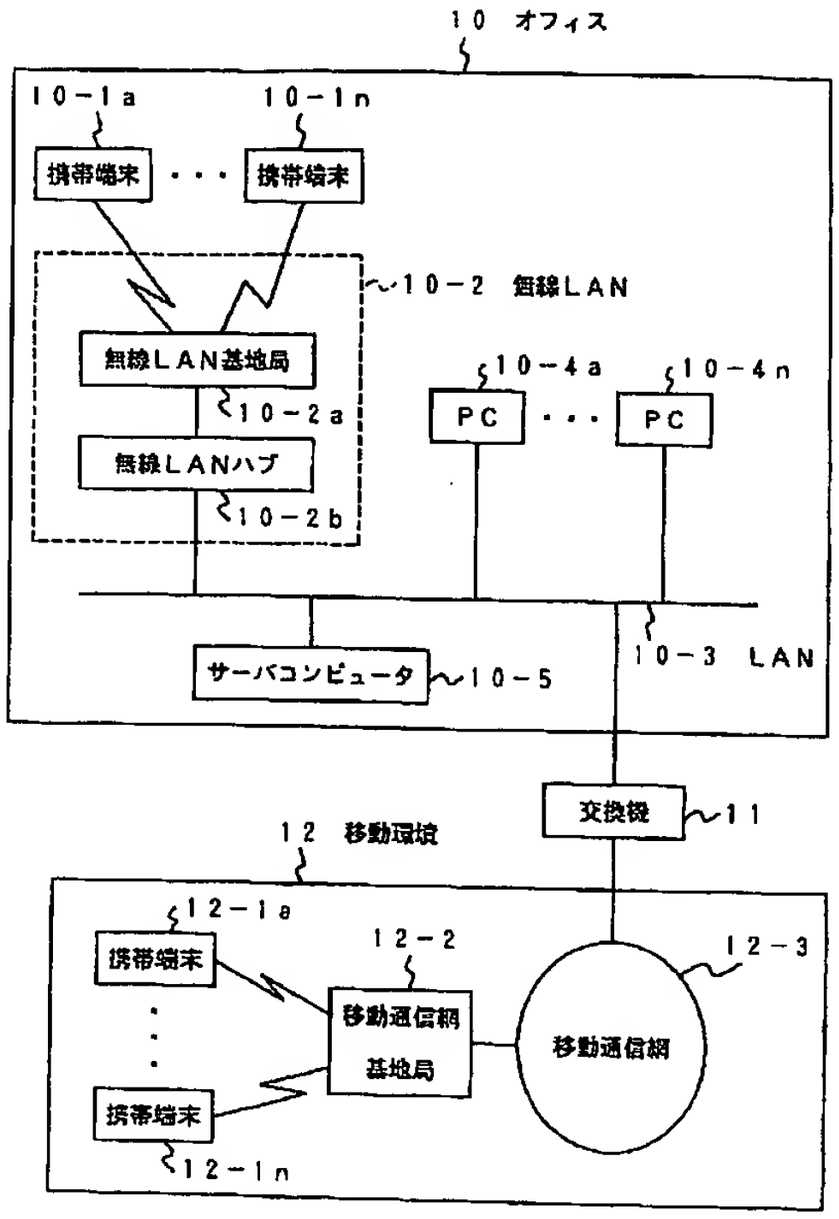
【図１２】



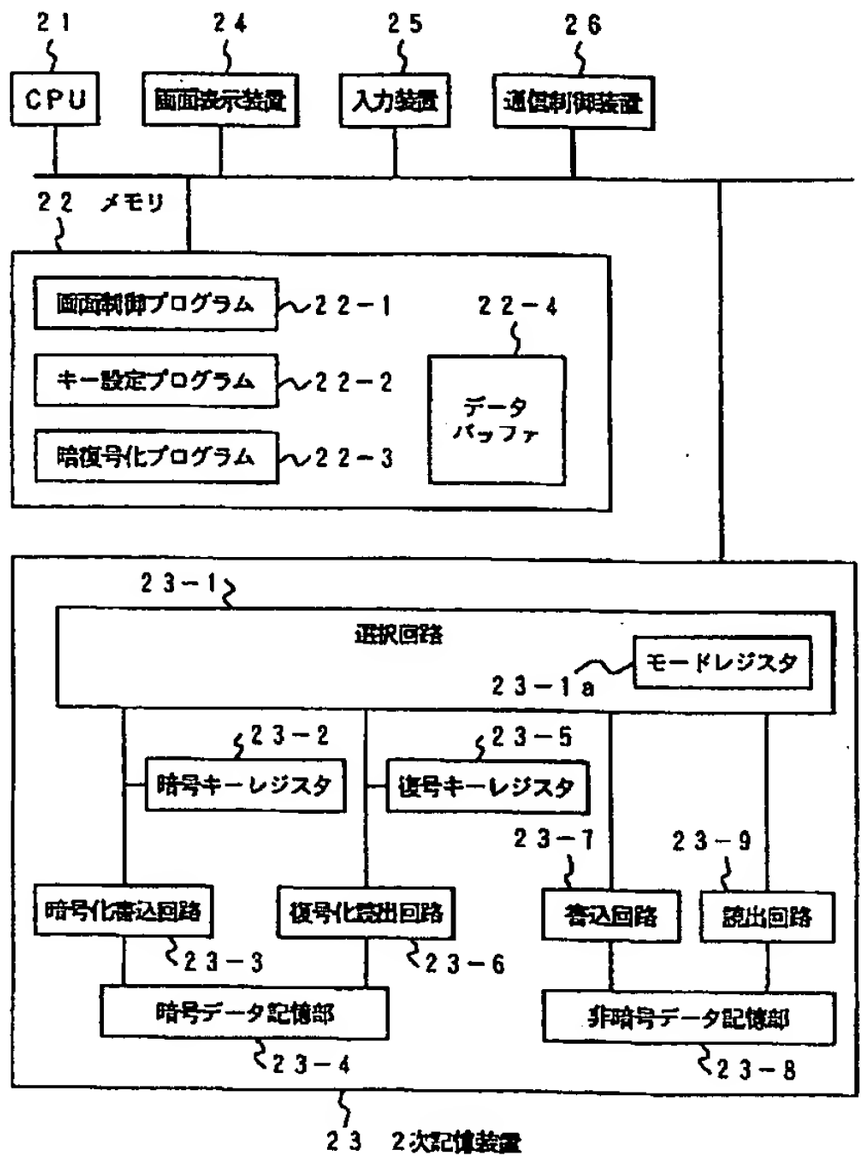
【図１９】



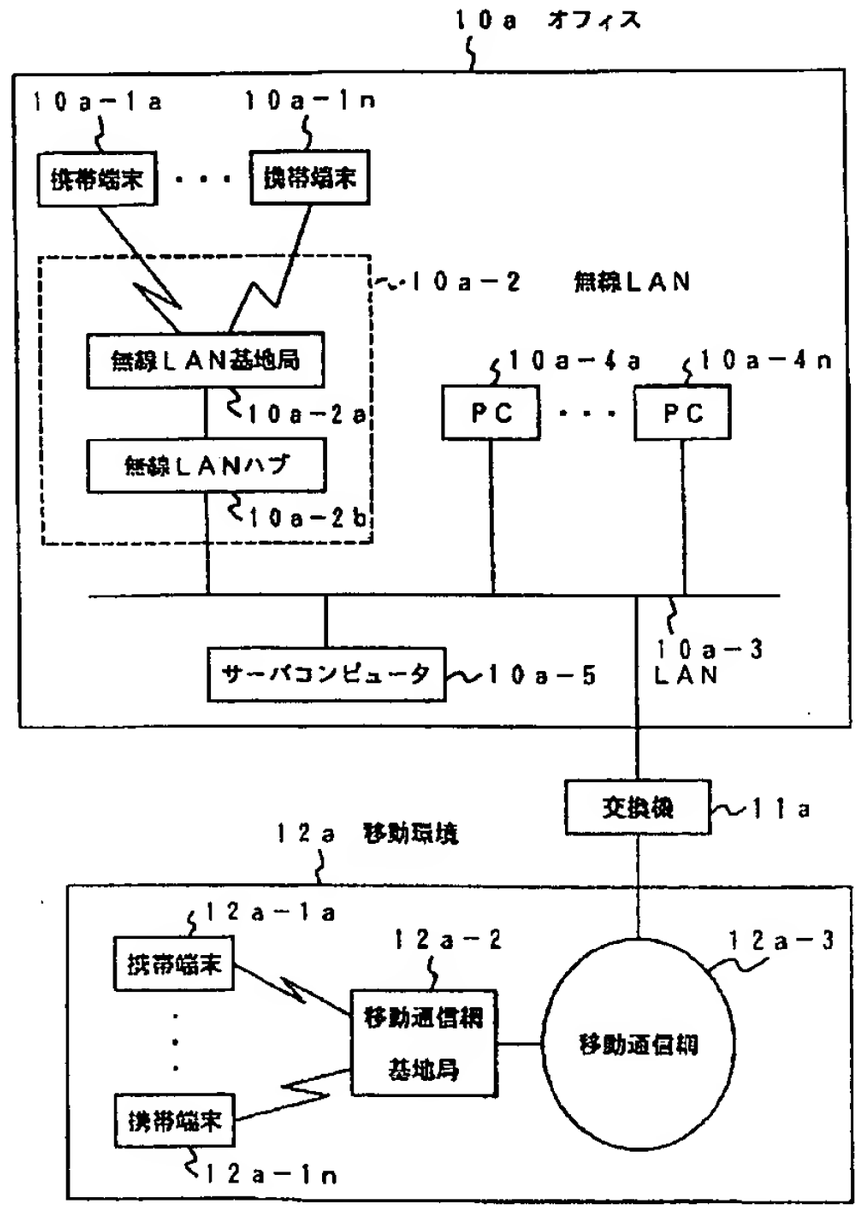
【図１】


１０　オフィス
１０－１ａ
１０－１ｎ
携帯端末
携帯端末
１０－２　無線ＬＡＮ
無線ＬＡＮ基地局
１０－２ａ
無線ＬＡＮハブ
１０－２ｂ
１０－４ａ
１０－４ｎ
ＰＣ
ＰＣ
サーバコンピュータ
１０－５
１０－３　ＬＡＮ
交換機
１１
１２　移動環境
１２－１ａ
携帯端末
１２－２
移動通信網
基地局
１２－３
移動通信網
携帯端末
１２－１ｎ

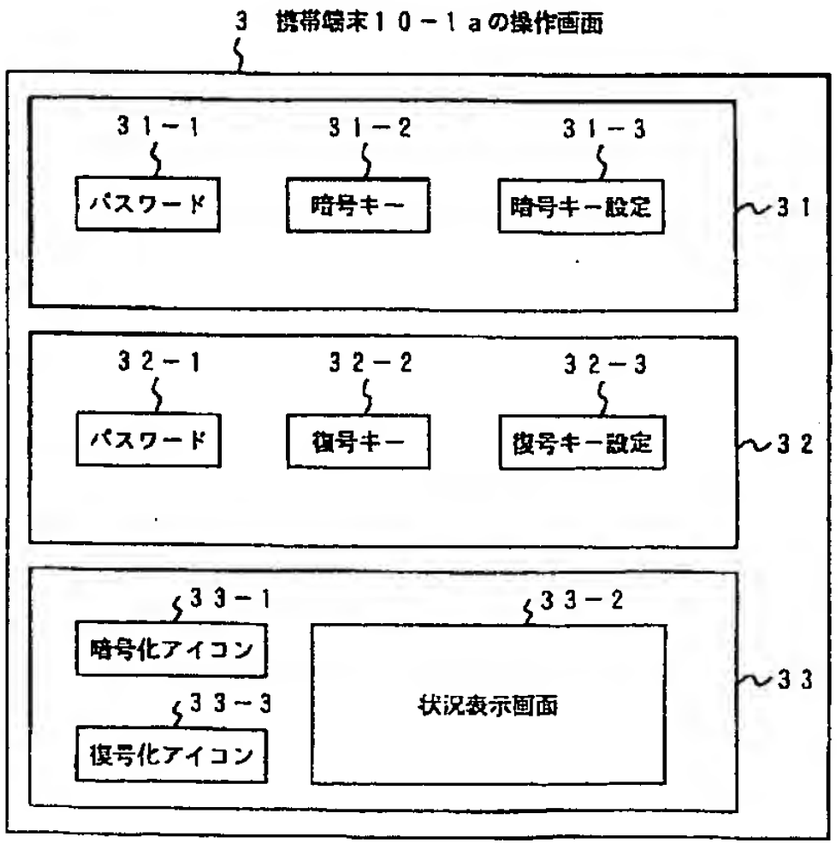
【図２】


２１
２４
２５
２６
ＣＰＵ
画面表示装置
入力装置
通信制御装置
２２　メモリ
画面制御プログラム
２２－１
２２－４
キー設定プログラム
２２－２
データバッファ
暗復号化プログラム
２２－３
２３－１
選択回路
２３－１ａ
モードレジスタ
２３－２
２３－５
暗号キーレジスタ
復号キーレジスタ
２３－７
２３－９
暗号化書込回路
復号化読出回路
書込回路
読出回路
２３－３
２３－６
暗号データ記憶部
非暗号データ記憶部
２３－４
２３－８
２３　２次記憶装置

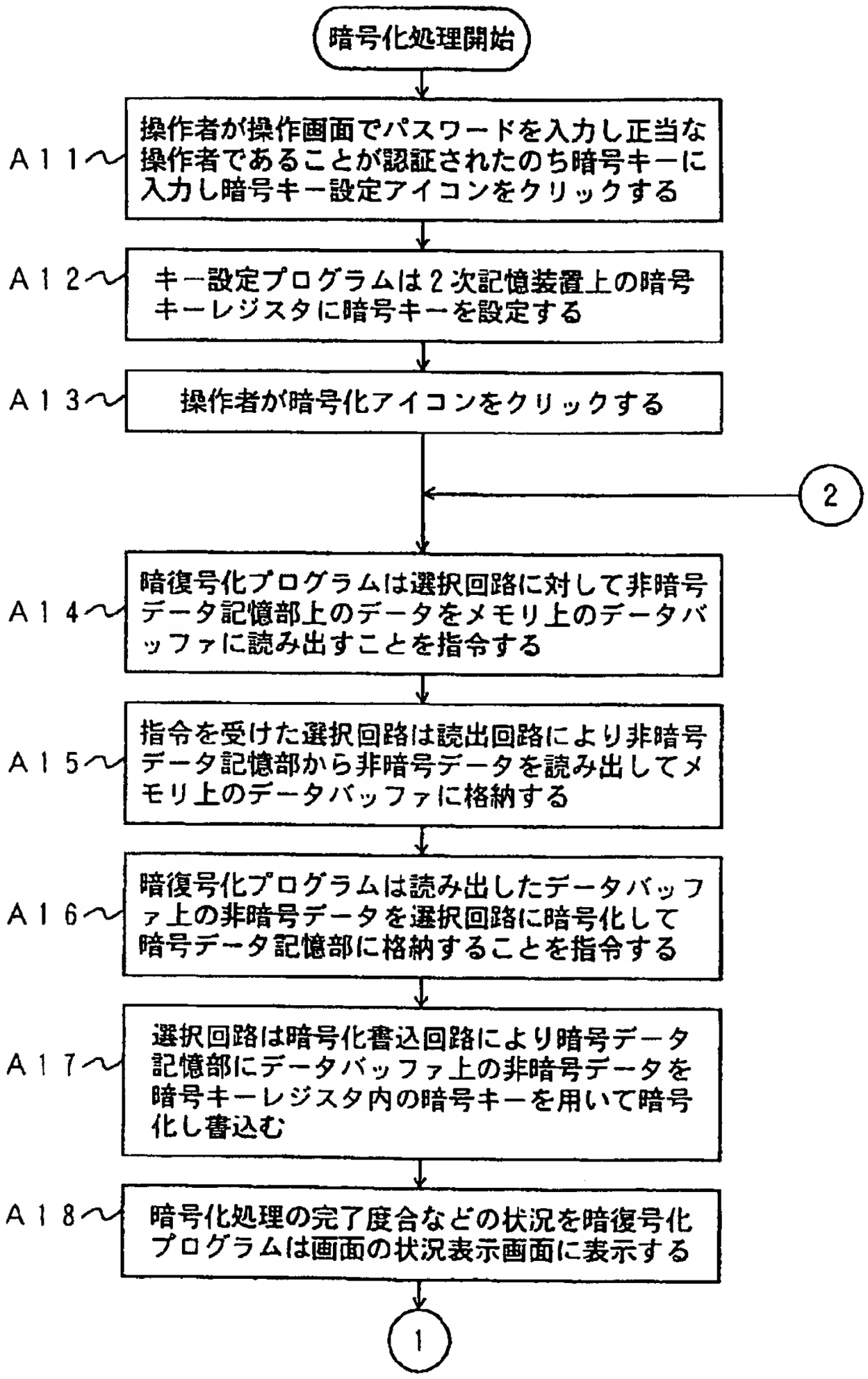
【図８】


１０ａ　オフィス
１０ａ－１ａ
１０ａ－１ｎ
携帯端末
携帯端末
１０ａ－２　無線ＬＡＮ
無線ＬＡＮ基地局
１０ａ－２ａ
無線ＬＡＮハブ
１０ａ－２ｂ
１０ａ－４ａ
１０ａ－４ｎ
ＰＣ
ＰＣ
サーバコンピュータ
１０ａ－５
１０ａ－３
ＬＡＮ
交換機
１１ａ
１２ａ　移動環境
１２ａ－１ａ
携帯端末
１２ａ－２
移動通信網
基地局
１２ａ－３
移動通信網
携帯端末
１２ａ－１ｎ

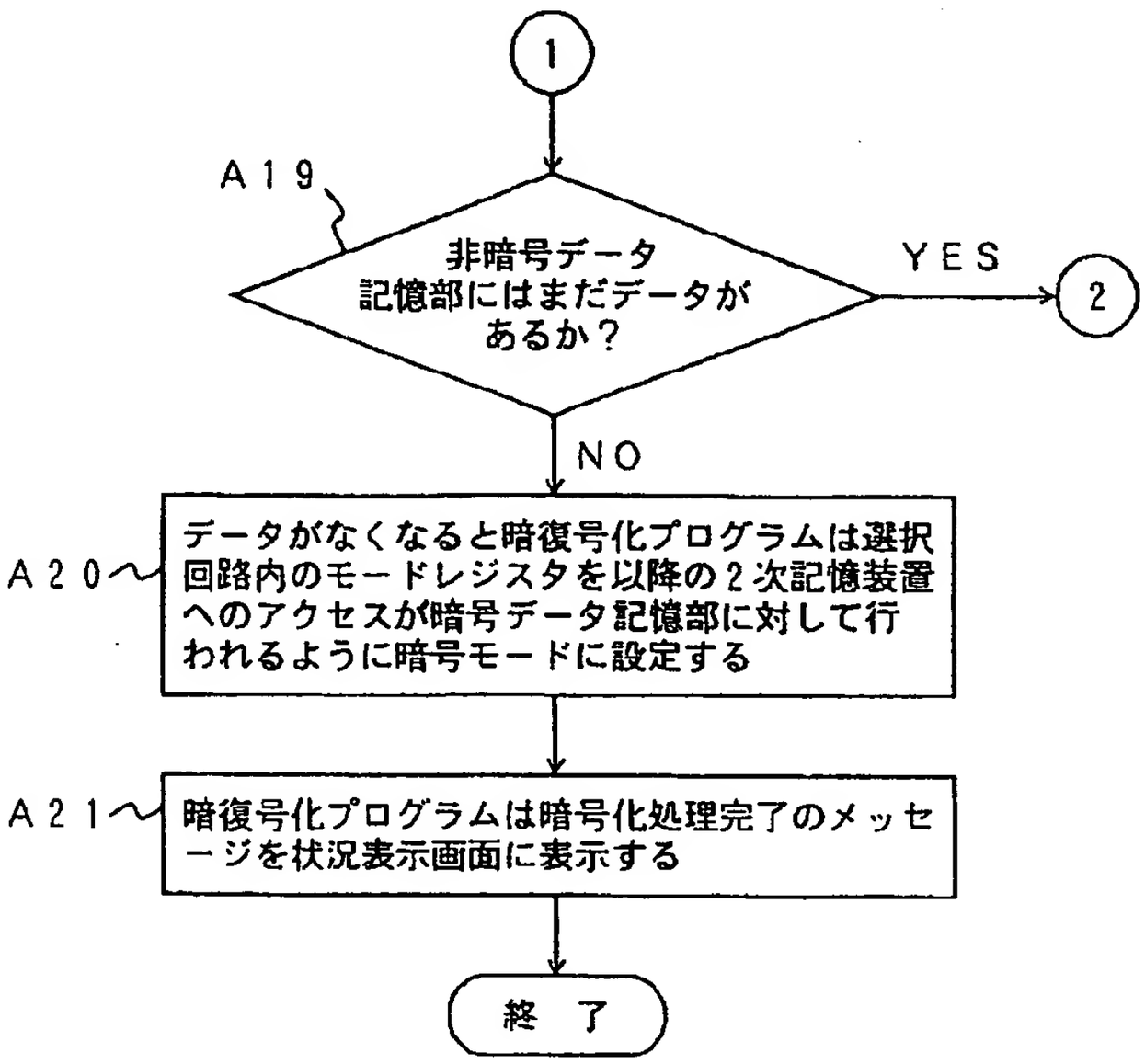
【図３】


３　携帯端末１０－１ａの操作画面
３１－１
３１－２
３１－３
パスワード
暗号キー
暗号キー設定
３１
３２－１
３２－２
３２－３
パスワード
復号キー
復号キー設定
３２
３３－１
３３－２
暗号化アイコン
状況表示画面
３３－３
復号化アイコン
３３

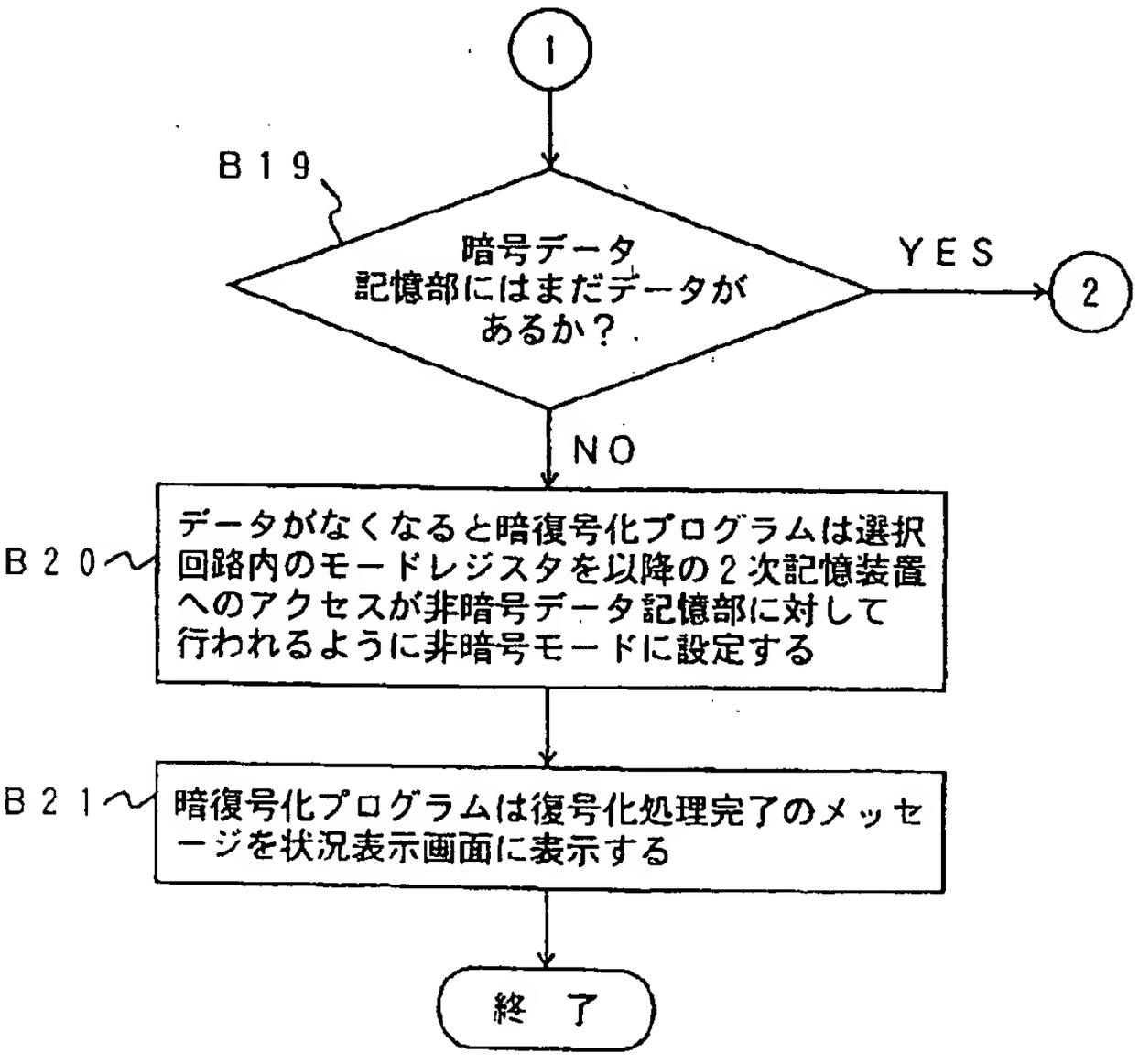
【図４】


暗号化処理開始
A１１
操作者が操作画面でパスワードを入力し正当な操作者であることが認証されたのち暗号キーに入力し暗号キー設定アイコンをクリックする
A１２
キー設定プログラムは２次記憶装置上の暗号キーレジスタに暗号キーを設定する
A１３
操作者が暗号化アイコンをクリックする
2
A１４
暗復号化プログラムは選択回路に対して非暗号データ記憶部上のデータをメモリ上のデータバッファに読み出すことを指令する
A１５
指令を受けた選択回路は読出回路により非暗号データ記憶部から非暗号データを読み出してメモリ上のデータバッファに格納する
A１６
暗復号化プログラムは読み出したデータバッファ上の非暗号データを選択回路に暗号化して暗号データ記憶部に格納することを指令する
A１７
選択回路は暗号化書込回路により暗号データ記憶部にデータバッファ上の非暗号データを暗号キーレジスタ内の暗号キーを用いて暗号化し書込む
A１８
暗号化処理の完了度合などの状況を暗復号化プログラムは画面の状況表示画面に表示する
1

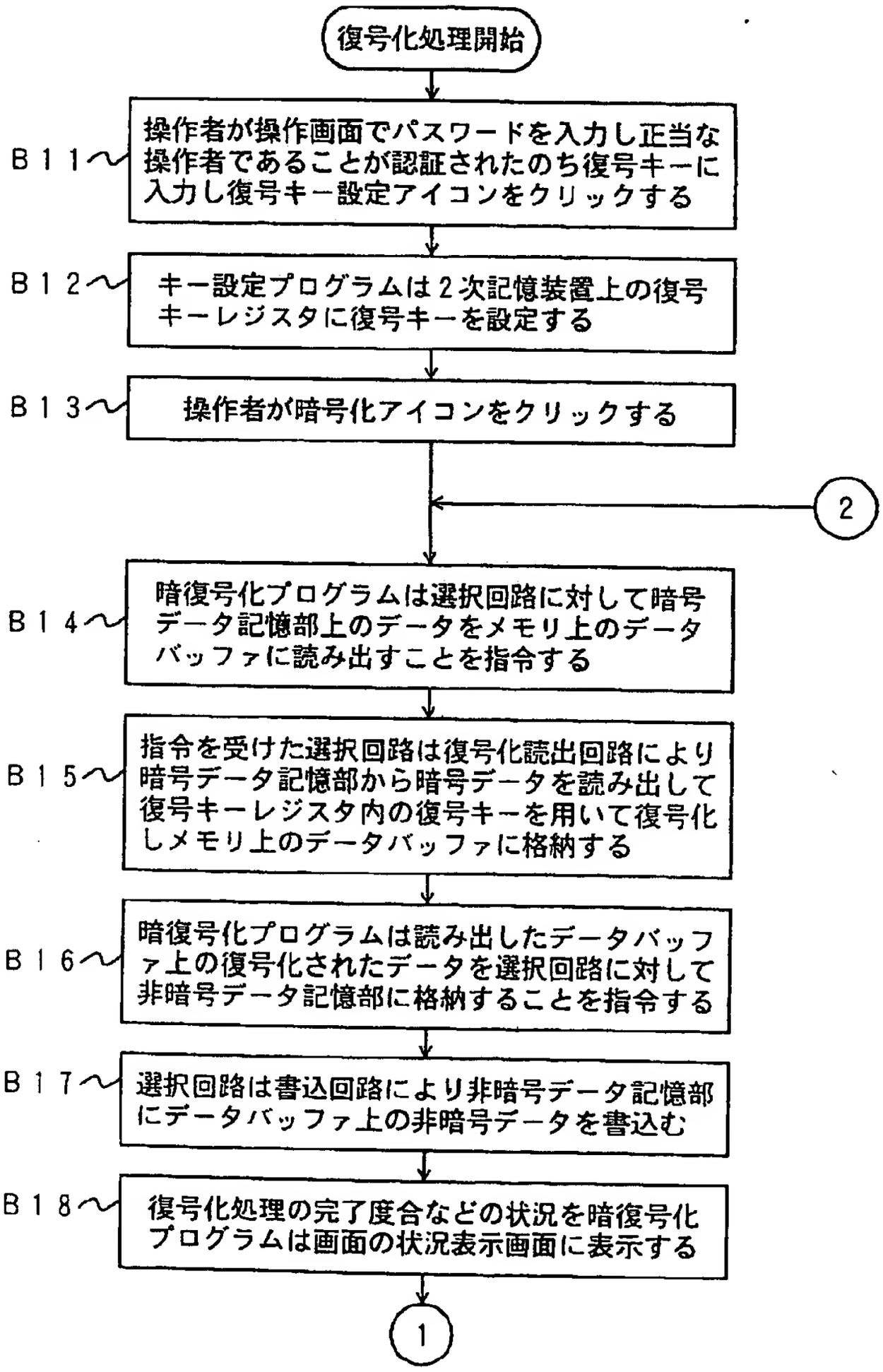
【図５】


1
A１９
非暗号データ
記憶部にはまだデータが
あるか？
YES
2
NO
A２０
データがなくなると暗復号化プログラムは選択
回路内のモードレジスタを以降の２次記憶装置
へのアクセスが暗号データ記憶部に対して行
われるように暗号モードに設定する
A２１
暗復号化プログラムは暗号化処理完了のメッセ
ージを状況表示画面に表示する
終　了

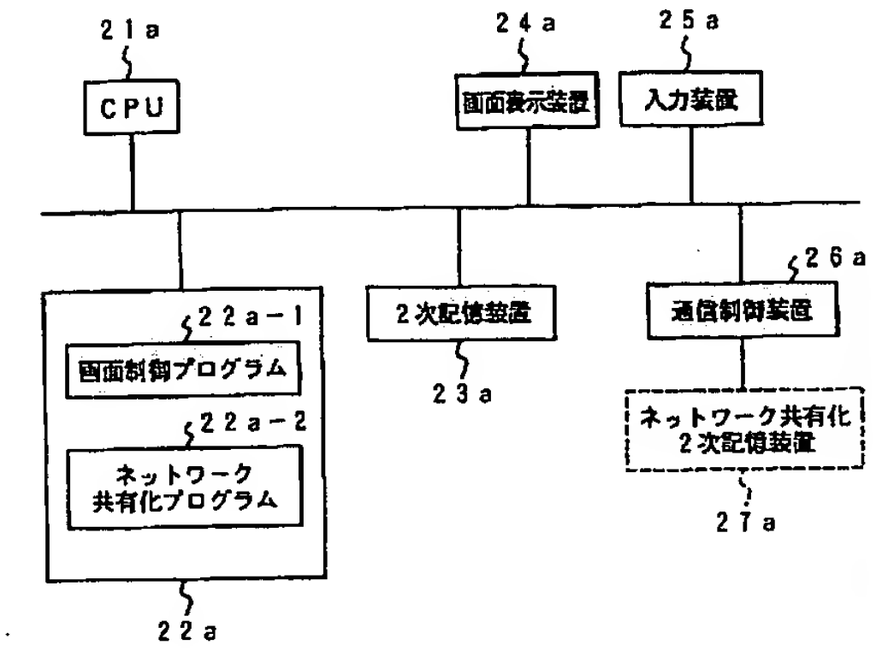
【図７】


1
B１９
暗号データ
記憶部にはまだデータが
あるか？
YES
2
NO
B２０
データがなくなると暗復号化プログラムは選択
回路内のモードレジスタを以降の２次記憶装置
へのアクセスが非暗号データ記憶部に対して
行われるように非暗号モードに設定する
B２１
暗復号化プログラムは復号化処理完了のメッセ
ージを状況表示画面に表示する
終　了

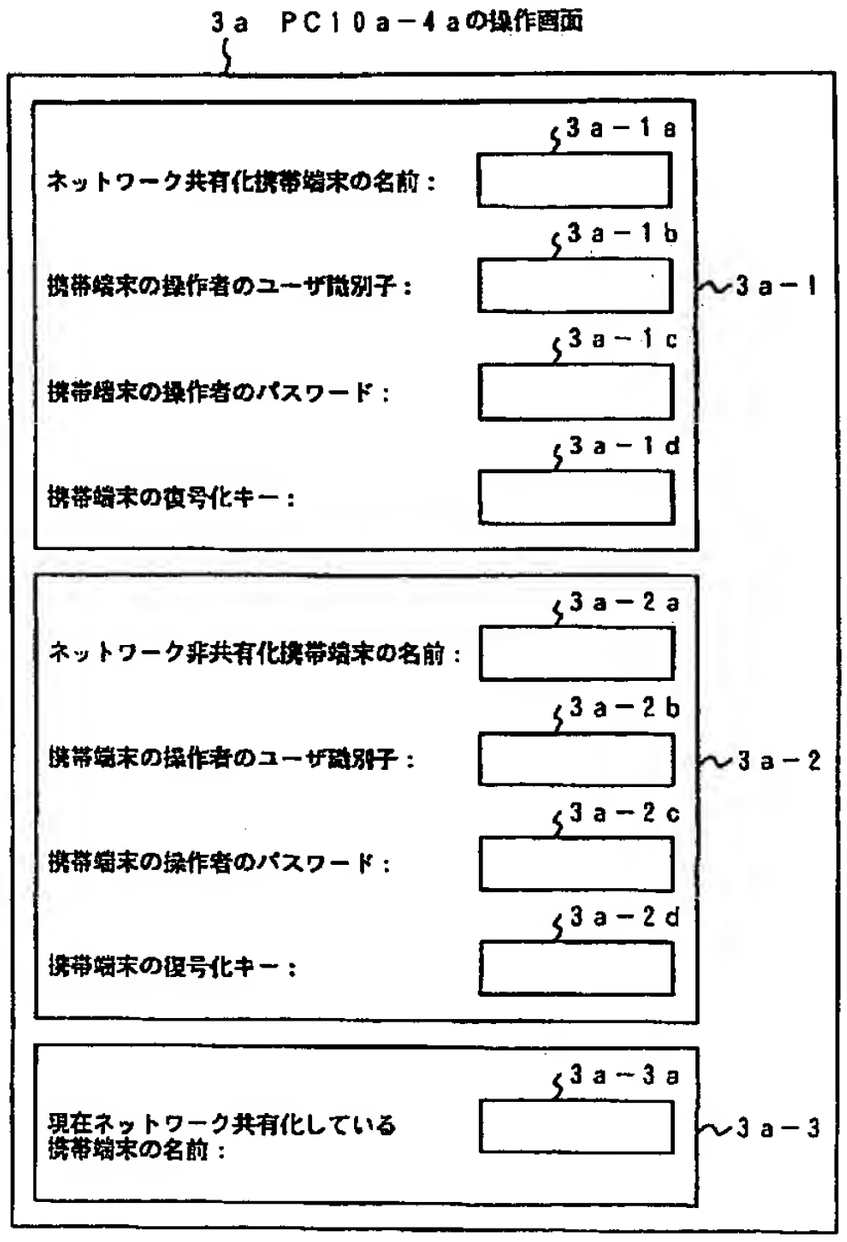
【図６】


復号化処理開始
B１１
操作者が操作画面でパスワードを入力し正当な操作者であることが認証されたのち復号キーに入力し復号キー設定アイコンをクリックする
B１２
キー設定プログラムは２次記憶装置上の復号キーレジスタに復号キーを設定する
B１３
操作者が暗号化アイコンをクリックする
2
B１４
暗復号化プログラムは選択回路に対して暗号データ記憶部上のデータをメモリ上のデータバッファに読み出すことを指令する
B１５
指令を受けた選択回路は復号化読出回路により暗号データ記憶部から暗号データを読み出して復号キーレジスタ内の復号キーを用いて復号化しメモリ上のデータバッファに格納する
B１６
暗復号化プログラムは読み出したデータバッファ上の復号化されたデータを選択回路に対して非暗号データ記憶部に格納することを指令する
B１７
選択回路は書込回路により非暗号データ記憶部にデータバッファ上の非暗号データを書込む
B１８
復号化処理の完了度合などの状況を暗復号化プログラムは画面の状況表示画面に表示する
1

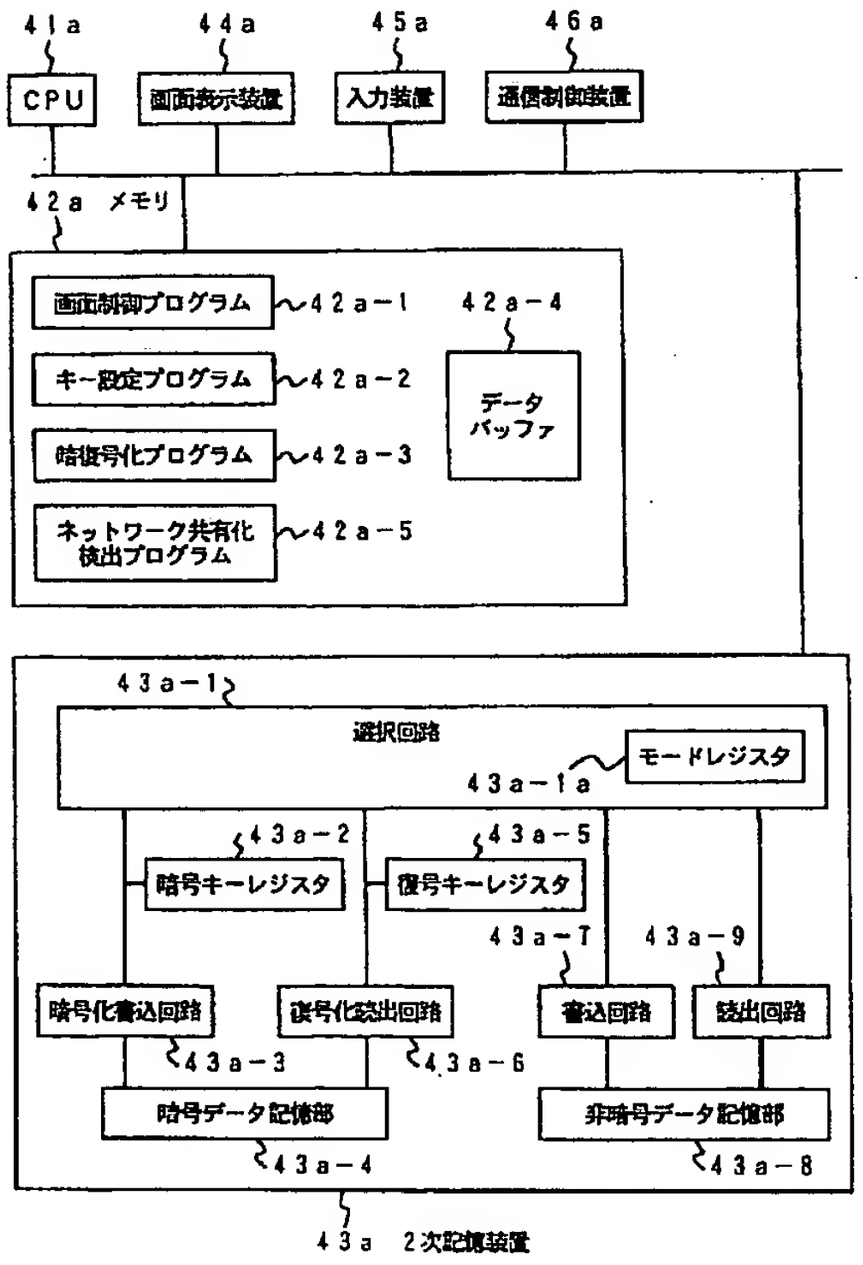
【図９】


21a
CPU
24a
画面表示装置
25a
入力装置
26a
通信制御装置
22a-1
画面制御プログラム
22a-2
ネットワーク
共有化プログラム
22a
23a
2次記憶装置
ネットワーク共有化
2次記憶装置
27a

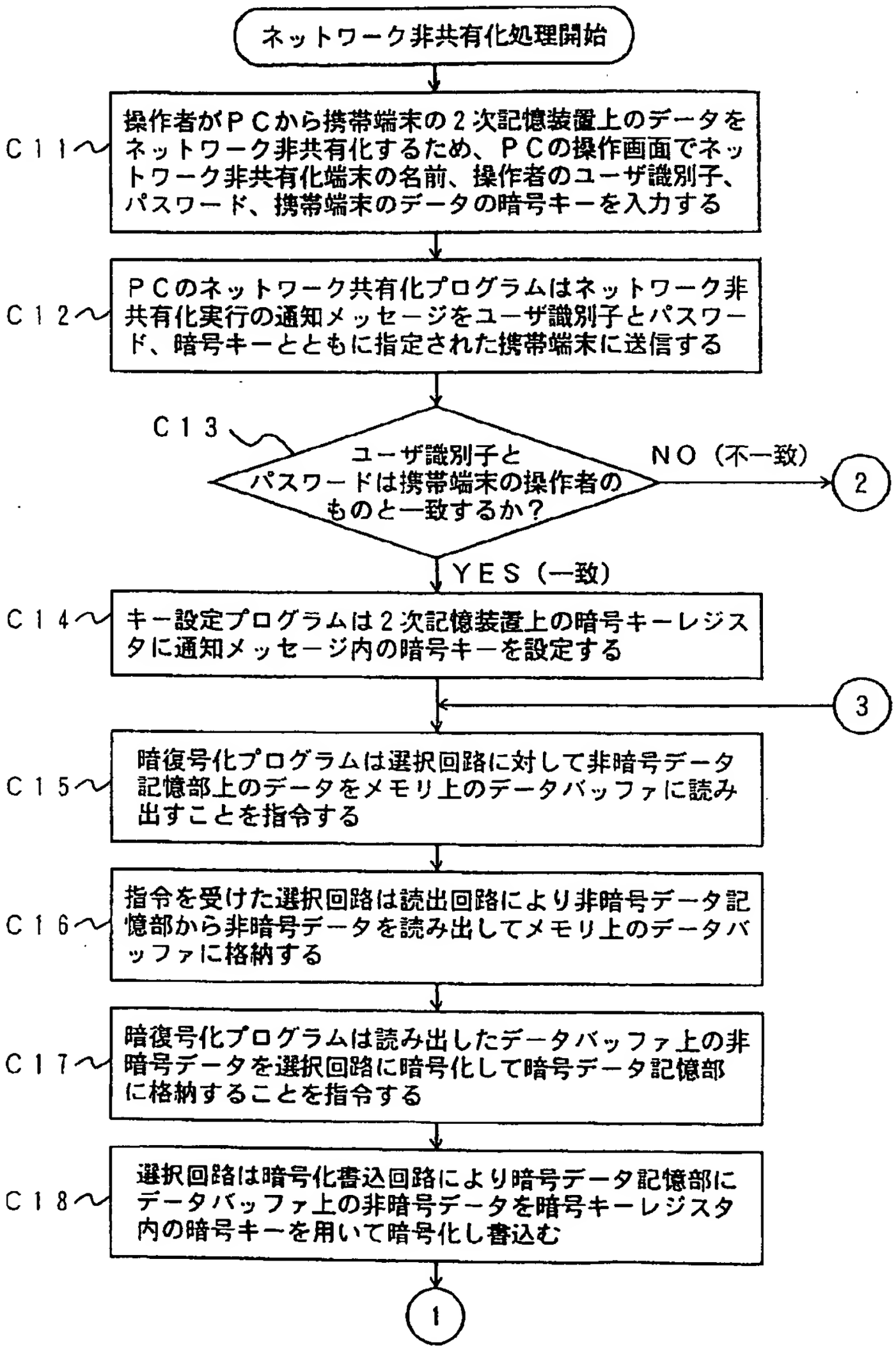
【図１０】


3a　PC10a－4aの操作画面
3a－1a
ネットワーク共有化携帯端末の名前：
3a－1b
携帯端末の操作者のユーザ識別子：
3a－1c
携帯端末の操作者のパスワード：
3a－1d
携帯端末の復号化キー：
3a－1
3a－2a
ネットワーク非共有化携帯端末の名前：
3a－2b
携帯端末の操作者のユーザ識別子：
3a－2c
携帯端末の操作者のパスワード：
3a－2d
携帯端末の復号化キー：
3a－2
3a－3a
現在ネットワーク共有化している
携帯端末の名前：
3a－3

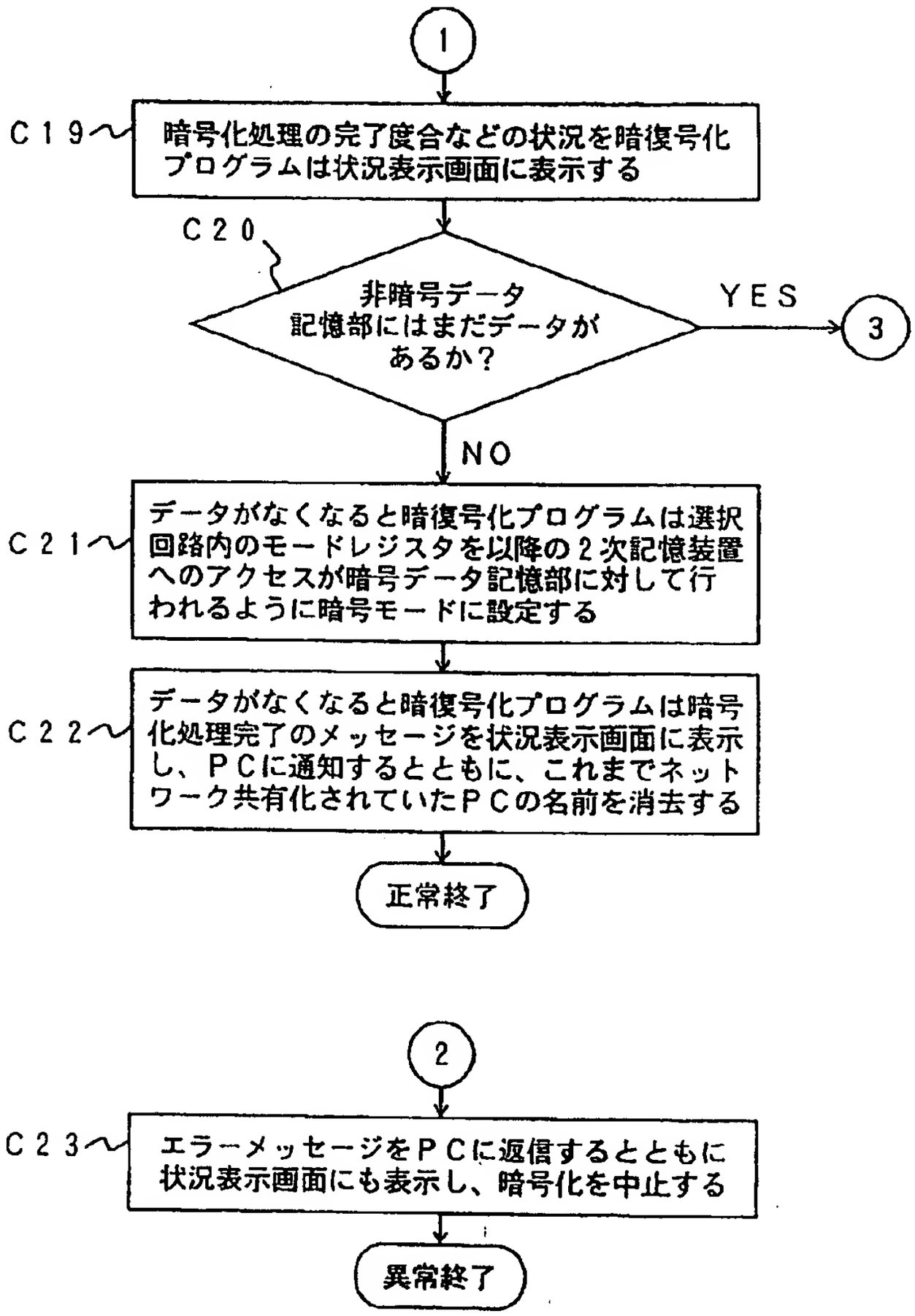
【図１１】


41a
CPU
44a
画面表示装置
45a
入力装置
46a
通信制御装置
42a　メモリ
画面制御プログラム
42a－1
キー設定プログラム
42a－2
暗復号化プログラム
42a－3
ネットワーク共有化
検出プログラム
42a－5
42a－4
データ
バッファ
43a－1
選択回路
モードレジスタ
43a－1a
43a－2
暗号キーレジスタ
43a－5
復号キーレジスタ
43a－7
43a－9
暗号化書込回路
43a－3
復号化読出回路
43a－6
書込回路
読出回路
暗号データ記憶部
43a－4
非暗号データ記憶部
43a－8
43a　2次記憶装置

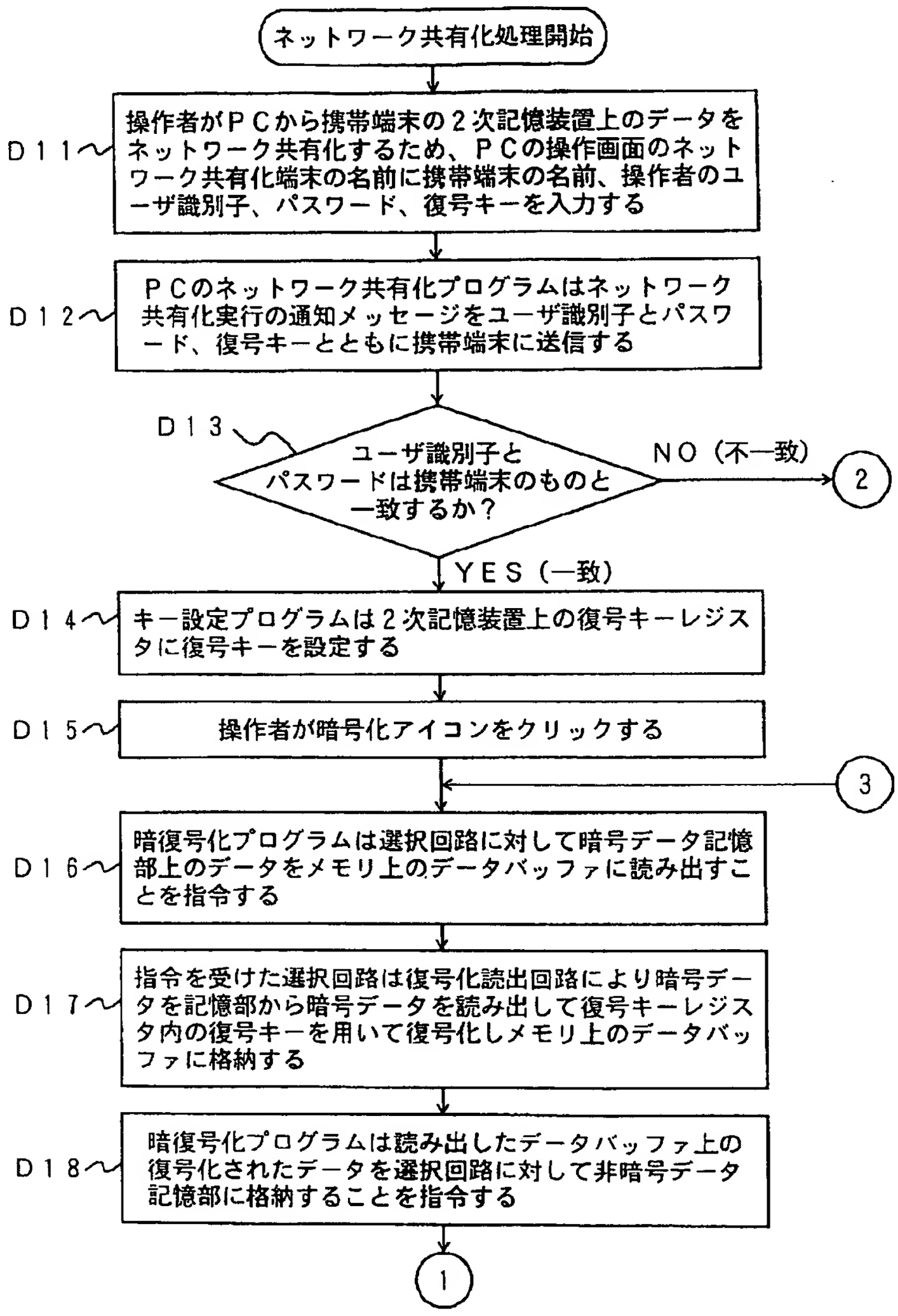
【図１３】


ネットワーク非共有化処理開始
C11
操作者がＰＣから携帯端末の２次記憶装置上のデータをネットワーク非共有化するため、ＰＣの操作画面でネットワーク非共有化端末の名前、操作者のユーザ識別子、パスワード、携帯端末のデータの暗号キーを入力する
C12
ＰＣのネットワーク共有化プログラムはネットワーク非共有化実行の通知メッセージをユーザ識別子とパスワード、暗号キーとともに指定された携帯端末に送信する
C13
ユーザ識別子とパスワードは携帯端末の操作者のものと一致するか？
ＮＯ（不一致）
2
ＹＥＳ（一致）
C14
キー設定プログラムは２次記憶装置上の暗号キーレジスタに通知メッセージ内の暗号キーを設定する
3
C15
暗復号化プログラムは選択回路に対して非暗号データ記憶部上のデータをメモリ上のデータバッファに読み出すことを指令する
C16
指令を受けた選択回路は読出回路により非暗号データ記憶部から非暗号データを読み出してメモリ上のデータバッファに格納する
C17
暗復号化プログラムは読み出したデータバッファ上の非暗号データを選択回路に暗号化して暗号データ記憶部に格納することを指令する
C18
選択回路は暗号化書込回路により暗号データ記憶部にデータバッファ上の非暗号データを暗号キーレジスタ内の暗号キーを用いて暗号化し書込む
1

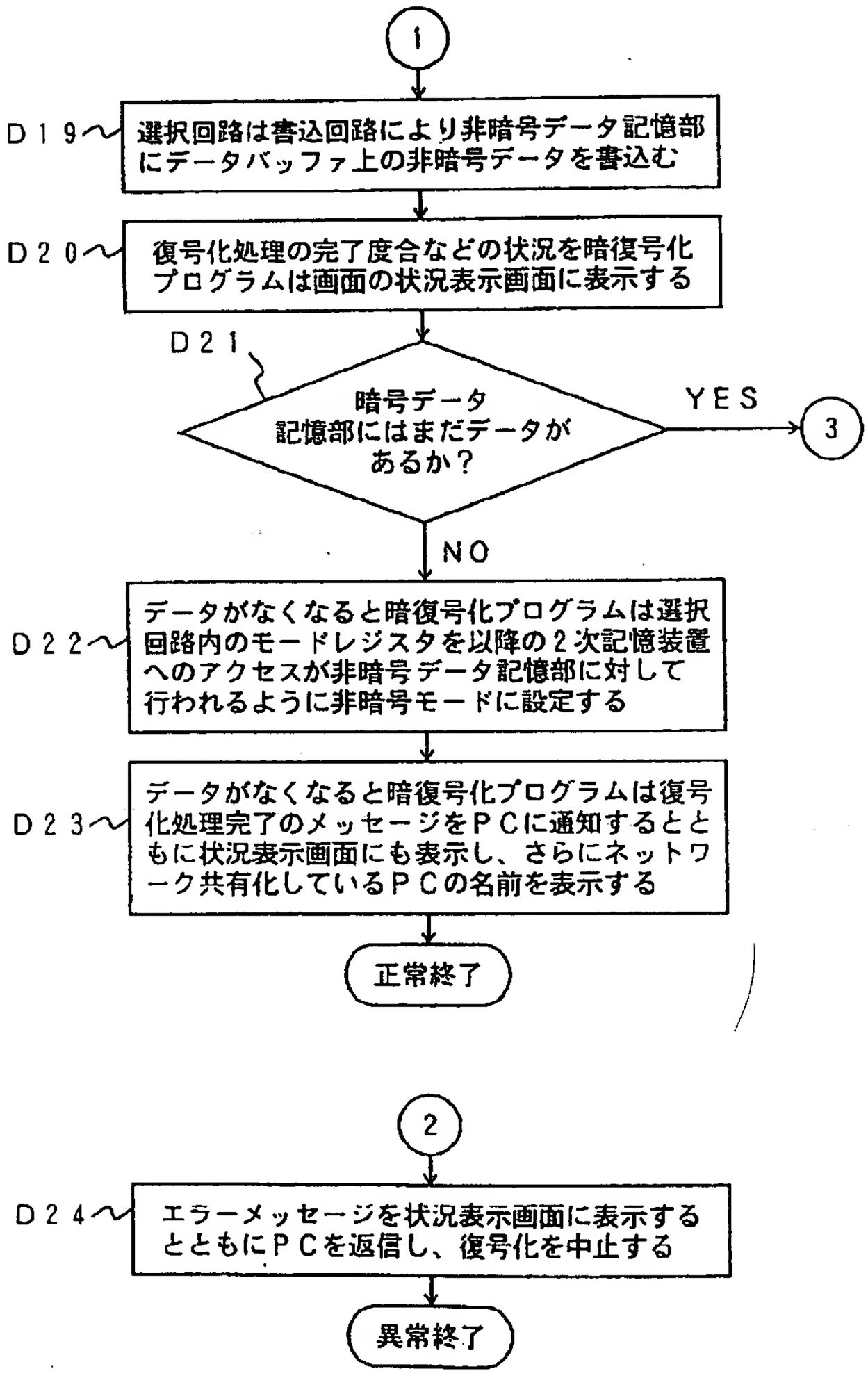
【図１４】


1
C１９
暗号化処理の完了度合などの状況を暗復号化プログラムは状況表示画面に表示する
C２０
非暗号データ記憶部にはまだデータがあるか？
YES
3
NO
C２１
データがなくなると暗復号化プログラムは選択回路内のモードレジスタを以降の２次記憶装置へのアクセスが暗号データ記憶部に対して行われるように暗号モードに設定する
C２２
データがなくなると暗復号化プログラムは暗号化処理完了のメッセージを状況表示画面に表示し、ＰＣに通知するとともに、これまでネットワーク共有化されていたＰＣの名前を消去する
正常終了
2
C２３
エラーメッセージをＰＣに返信するとともに状況表示画面にも表示し、暗号化を中止する
異常終了

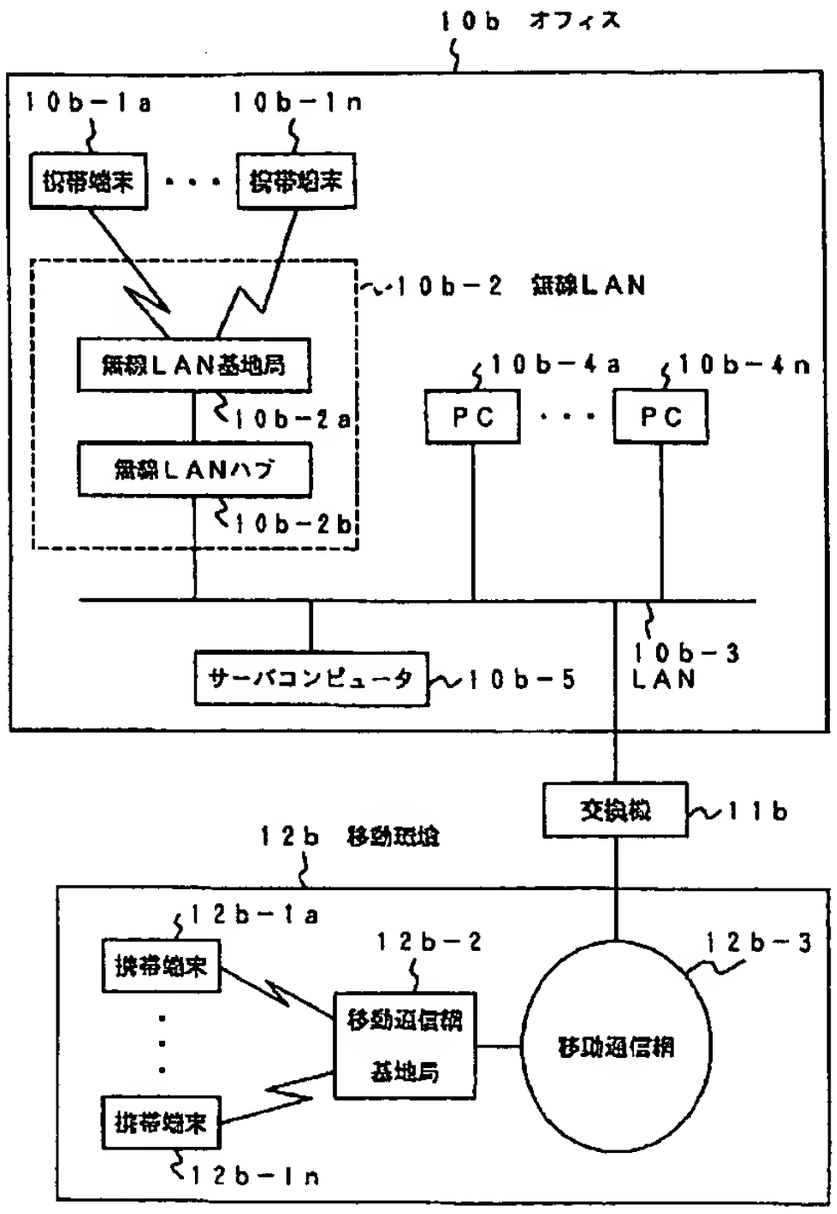
【図１５】


ネットワーク共有化処理開始
D１１
操作者がＰＣから携帯端末の２次記憶装置上のデータをネットワーク共有化するため、ＰＣの操作画面のネットワーク共有化端末の名前に携帯端末の名前、操作者のユーザ識別子、パスワード、復号キーを入力する
D１２
ＰＣのネットワーク共有化プログラムはネットワーク共有化実行の通知メッセージをユーザ識別子とパスワード、復号キーとともに携帯端末に送信する
D１３
ユーザ識別子とパスワードは携帯端末のものと一致するか？
ＮＯ（不一致）
2
ＹＥＳ（一致）
D１４
キー設定プログラムは２次記憶装置上の復号キーレジスタに復号キーを設定する
D１５
操作者が暗号化アイコンをクリックする
3
D１６
暗復号化プログラムは選択回路に対して暗号データ記憶部上のデータをメモリ上のデータバッファに読み出すことを指令する
D１７
指令を受けた選択回路は復号化読出回路により暗号データを記憶部から暗号データを読み出して復号キーレジスタ内の復号キーを用いて復号化しメモリ上のデータバッファに格納する
D１８
暗復号化プログラムは読み出したデータバッファ上の復号化されたデータを選択回路に対して非暗号データ記憶部に格納することを指令する
1

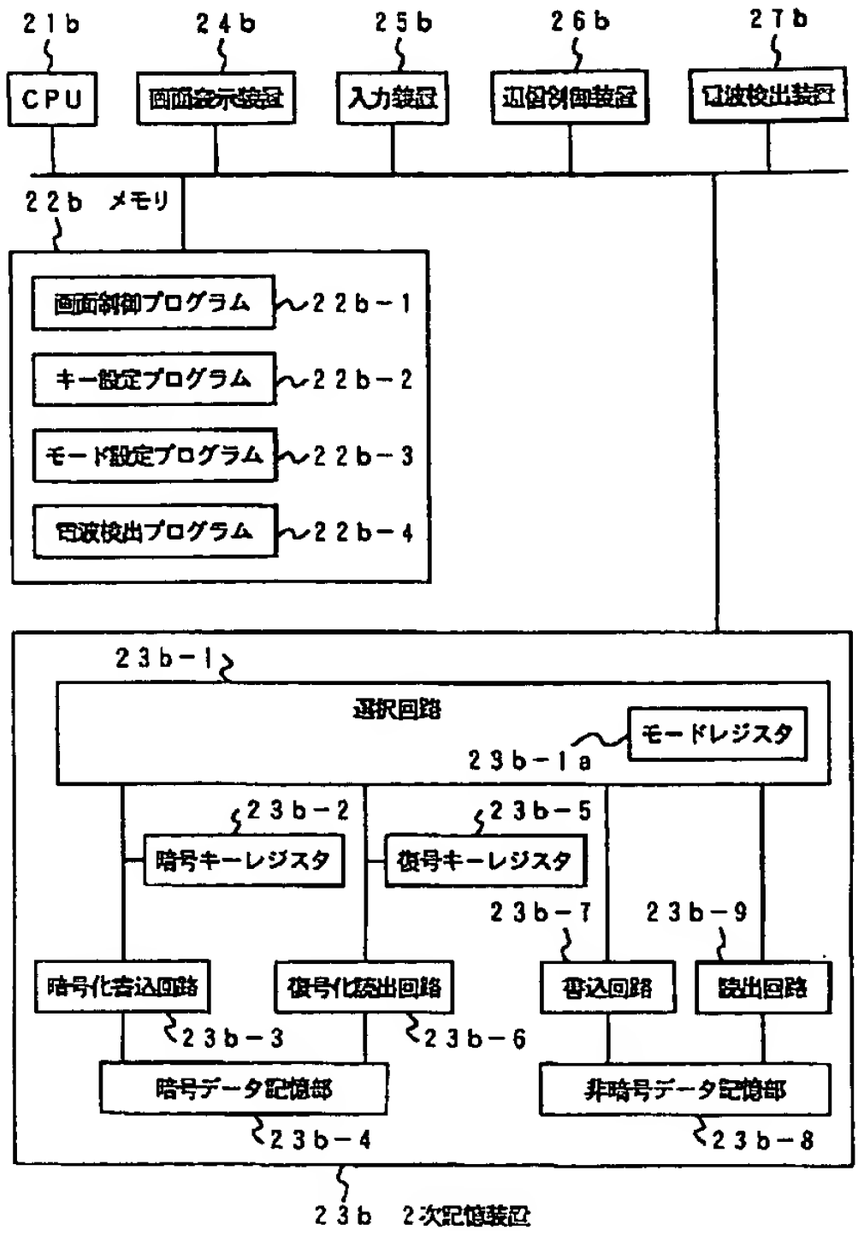
【図１６】


1
D１９
選択回路は書込回路により非暗号データ記憶部にデータバッファ上の非暗号データを書込む
D２０
復号化処理の完了度合などの状況を暗復号化プログラムは画面の状況表示画面に表示する
D２１
暗号データ記憶部にはまだデータがあるか？
YES
3
NO
D２２
データがなくなると暗復号化プログラムは選択回路内のモードレジスタを以降の２次記憶装置へのアクセスが非暗号データ記憶部に対して行われるように非暗号モードに設定する
D２３
データがなくなると暗復号化プログラムは復号化処理完了のメッセージをＰＣに通知するとともに状況表示画面にも表示し、さらにネットワーク共有化しているＰＣの名前を表示する
正常終了
2
D２４
エラーメッセージを状況表示画面に表示するとともにＰＣを返信し、復号化を中止する
異常終了

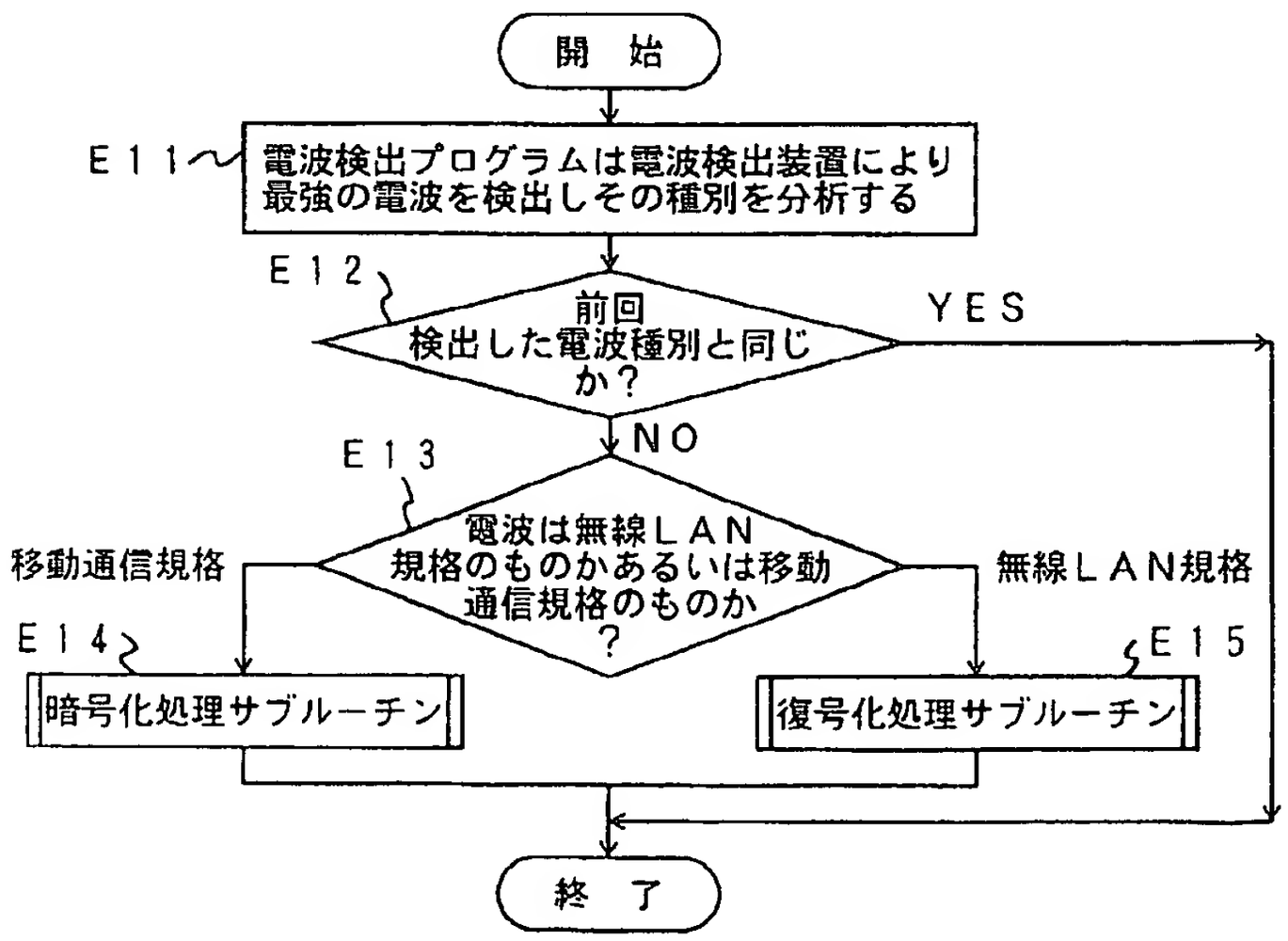
【図１７】


10b　オフィス
10b-1a
10b-1n
携帯端末
携帯端末
10b-2　無線LAN
無線LAN基地局
10b-2a
無線LANハブ
10b-2b
10b-4a
10b-4n
PC
PC
サーバコンピュータ
10b-5
10b-3
LAN
交換機
11b
12b　移動環境
12b-1a
携帯端末
12b-2
移動通信網
基地局
12b-3
移動通信網
携帯端末
12b-1n

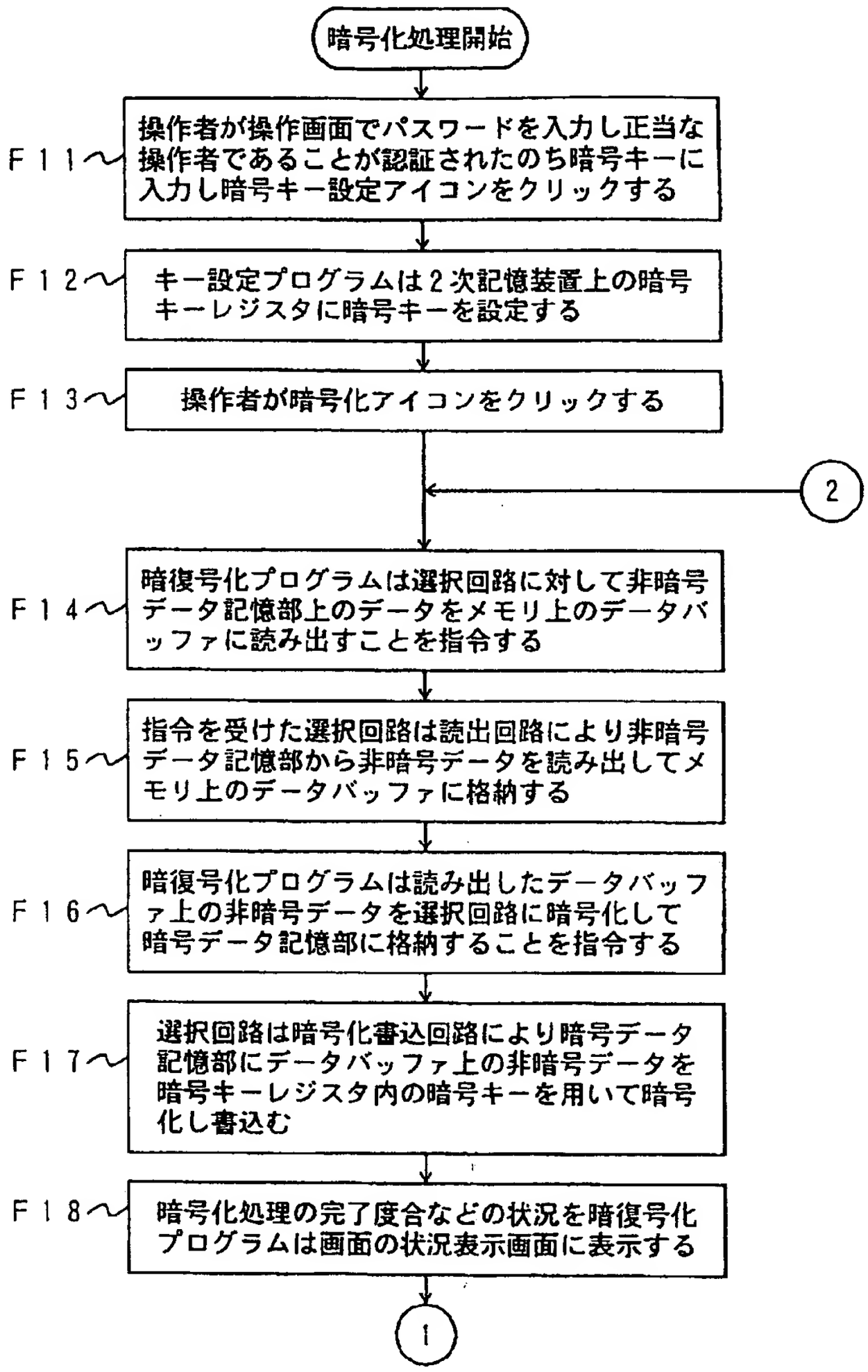
【図１８】


21b
24b
25b
26b
27b
CPU
画面表示装置
入力装置
通信制御装置
電波検出装置
22b　メモリ
画面制御プログラム
22b-1
キー設定プログラム
22b-2
モード設定プログラム
22b-3
電波検出プログラム
22b-4
23b-1
選択回路
モードレジスタ
23b-1a
23b-2
暗号キーレジスタ
23b-5
復号キーレジスタ
23b-7
23b-9
暗号化書込回路
復号化読出回路
書込回路
読出回路
23b-3
23b-6
暗号データ記憶部
非暗号データ記憶部
23b-4
23b-8
23b　2次記憶装置

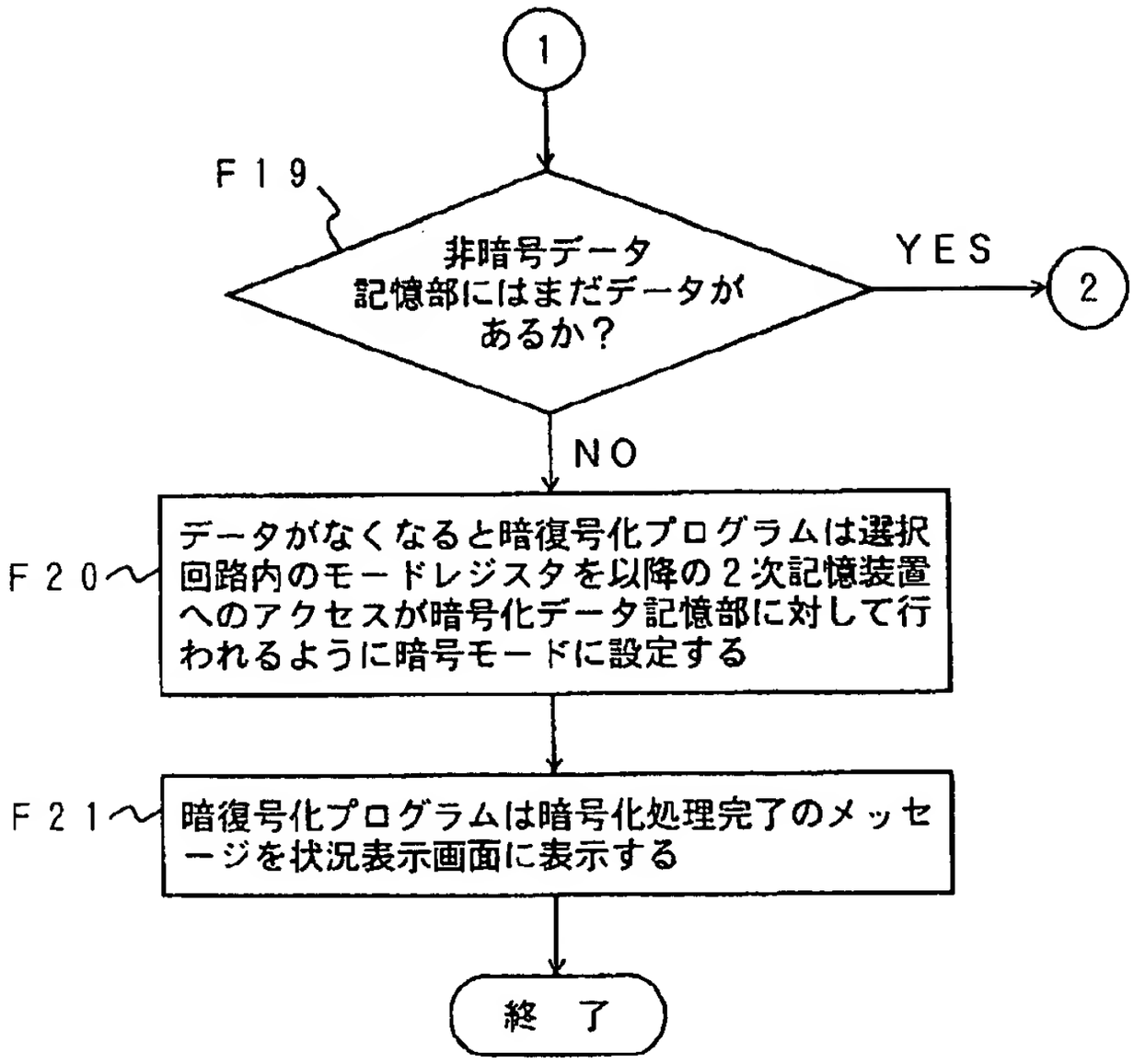
【図２０】


開　始
E11
電波検出プログラムは電波検出装置により最強の電波を検出しその種別を分析する
E12
前回検出した電波種別と同じか？
YES
NO
E13
電波は無線ＬＡＮ規格のものかあるいは移動通信規格のものか？
移動通信規格
無線ＬＡＮ規格
E14
暗号化処理サブルーチン
E15
復号化処理サブルーチン
終　了

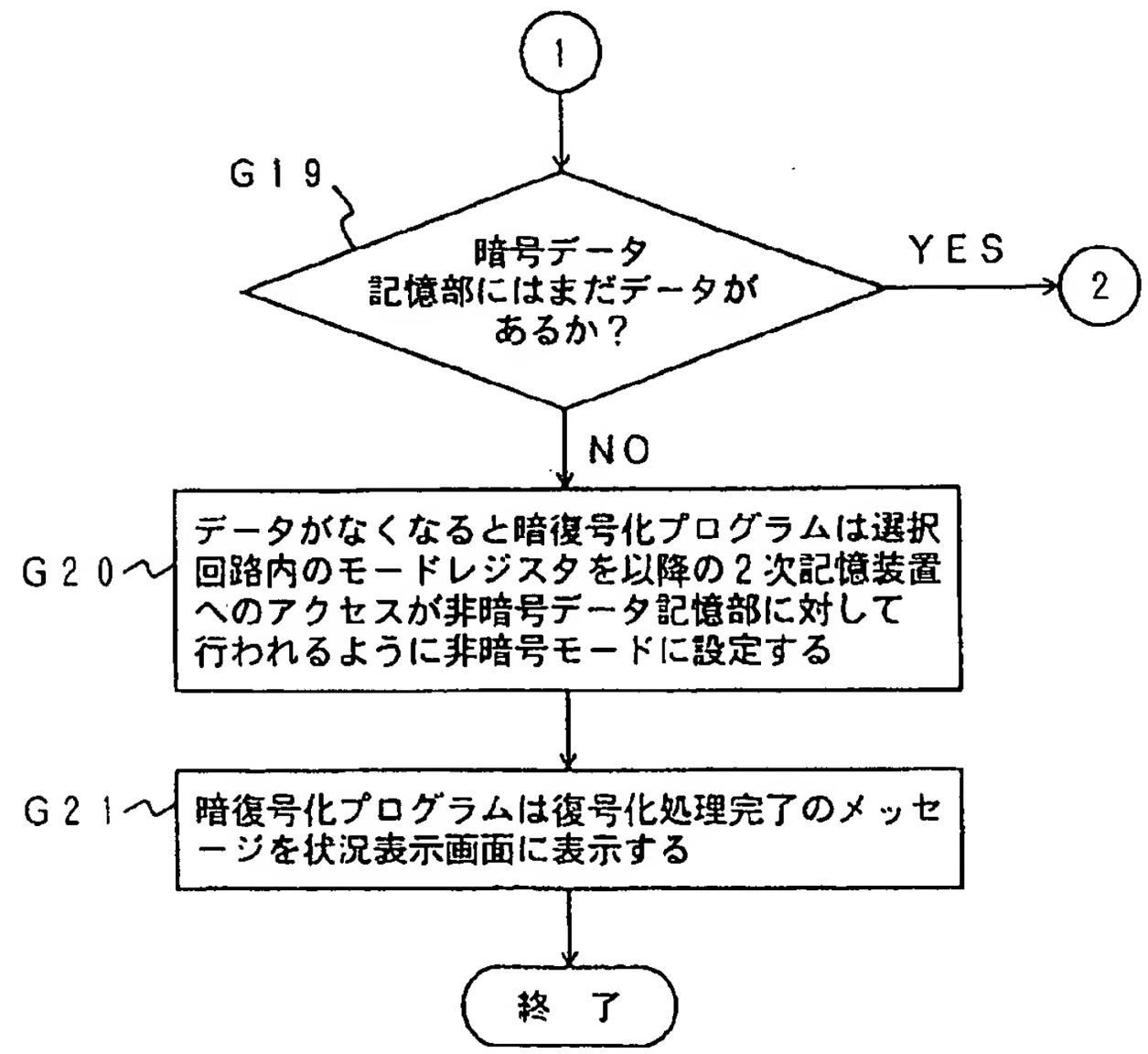
【図２１】


暗号化処理開始
F１１
操作者が操作画面でパスワードを入力し正当な操作者であることが認証されたのち暗号キーに入力し暗号キー設定アイコンをクリックする
F１２
キー設定プログラムは２次記憶装置上の暗号キーレジスタに暗号キーを設定する
F１３
操作者が暗号化アイコンをクリックする
2
F１４
暗復号化プログラムは選択回路に対して非暗号データ記憶部上のデータをメモリ上のデータバッファに読み出すことを指令する
F１５
指令を受けた選択回路は読出回路により非暗号データ記憶部から非暗号データを読み出してメモリ上のデータバッファに格納する
F１６
暗復号化プログラムは読み出したデータバッファ上の非暗号データを選択回路に暗号化して暗号データ記憶部に格納することを指令する
F１７
選択回路は暗号化書込回路により暗号データ記憶部にデータバッファ上の非暗号データを暗号キーレジスタ内の暗号キーを用いて暗号化し書込む
F１８
暗号化処理の完了度合などの状況を暗復号化プログラムは画面の状況表示画面に表示する
1

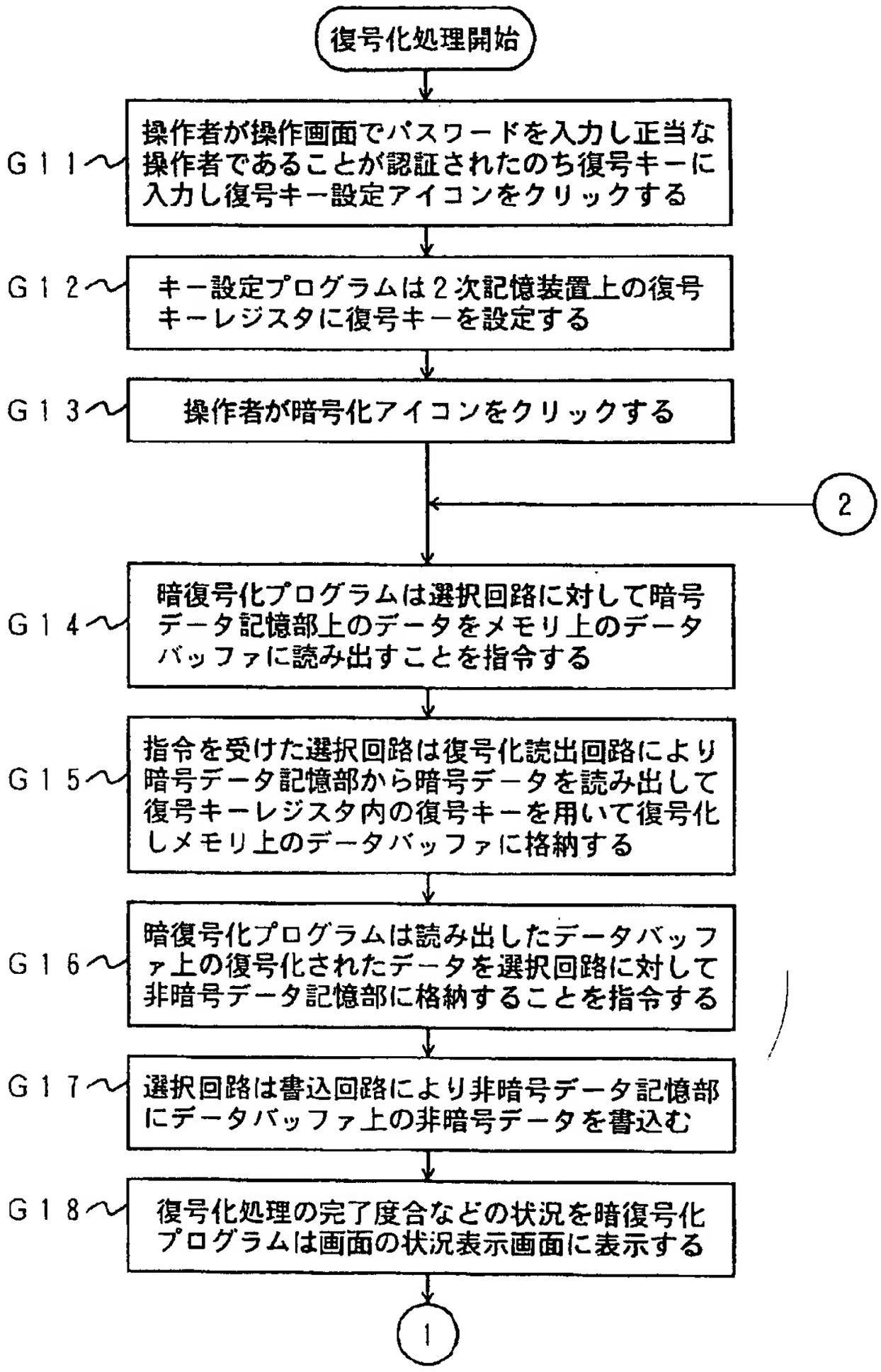
【図２２】


1
F１９
非暗号データ
記憶部にはまだデータが
あるか？
YES
2
NO
F２０
データがなくなると暗復号化プログラムは選択
回路内のモードレジスタを以降の２次記憶装置
へのアクセスが暗号化データ記憶部に対して行
われるように暗号モードに設定する
F２１
暗復号化プログラムは暗号化処理完了のメッセ
ージを状況表示画面に表示する
終　了

【図２４】


1
G１９
暗号データ
記憶部にはまだデータが
あるか？
YES
2
NO
G２０
データがなくなると暗復号化プログラムは選択
回路内のモードレジスタを以降の２次記憶装置
へのアクセスが非暗号データ記憶部に対して
行われるように非暗号モードに設定する
G２１
暗復号化プログラムは復号化処理完了のメッセ
ージを状況表示画面に表示する
終　了

【図２３】



フロントページの続き

(51)Int.Cl.[6]	識別記号	FI	
H04L 12/28		H04L 11/00	310B